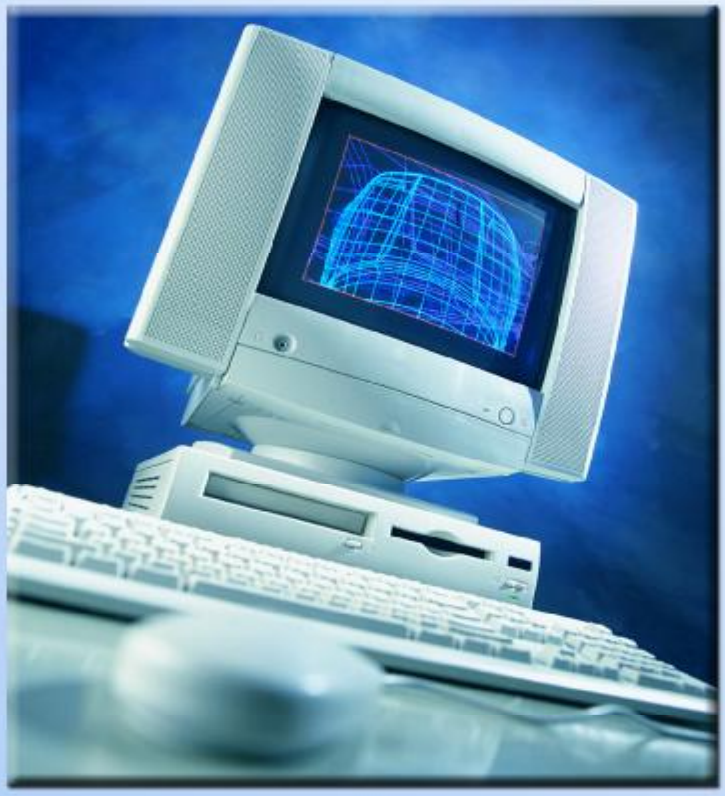
بخش سوم : اینترنت **صفحه**

بخش چهارم شبکه **صفحه**

بخش سوم: اینترنت



معرفی شبکه پهناور جهانی (World Wide Web)

قبل از بوجود آمدن اینترنت و وب، رویای زاندا مطرح بود. در این رویا تمامی علوم، مستندات، تصاویر، صوت، ویدئو و... توسط هر فرد که دارای یکدستگاه کامپیوتر بود در هر زمان و مکان د لخواه، قابل دستیابی بود. زاندا، رویای" تدنلسون " از یک کامپیوتر خیالی بود. وی دنیائی را که در آن اطلاعات از طریق ابر متن ها و ابر رسانه ها بصورت یک شبکه تار عنکبوتی بهم متصل و مرتبط می گردیدند، پیش بینی کرده بود. در این دنیا اطلاعات بصورت یک کتابخانه جهانی در نظر گرفته می شوند. دستیابی به این کتابخانه جهانی و استفاده از آن تاثیر شگرفی در جوامع متفاوت بشری را بدنبال داشته و منشا بروز تحولات عظیم در حیات بشری خواهد بود.

نحوه شکل گیری و بوجود آمدن وب

زاندا یک رویا بود، ولی امروز با واقعیتی بنام وب مواجه هستیم. به کمک وب اطلاعات موجود، صرفنظر از محل استقرار بهم پیوند خورده و امکان دستیابی به دریائی از اطلاعات برای استفاده کننده فراهم میگردد. اطلاعات فوق دارای ماهیتی کاملا" پویا می باشند. اطلاعات موجود در یک دایره المعارف بصورت ایستا می باشند ولی اطلاعات موجود در وب بصورت پویا بوده و دائما" بهنگام میشوند. با استفاده از وب میتوان در سریعترین زمان ممکن به جدیدترین اطلاعات دستیابی پیدا کرد.اطلاعات فوق از طریق سایت های متعدد که هر کدام می توانند در یک و یا چندین محل مستقر یاشند در اختیار استفاده کننده قرار میگیرد. وب پتانسیل بالای خود را مدیون دو تکنولوژی مدرن: " ابر متن ها"(HyperText) و" ابر رسانه ها " (HyperMedia) است. در ابرمتن ها، اطلاعات مرتبط با استفاده از یک روش مدون بهم پیوند زده میشوند. با استفاده از ارتباطات تعریف شده بین اطلاعات، میتوان با هر روش دلخواه و طی یک مسیر خطی و یا غیر خطی به اطلاعات مورد نظر دستیابی پیدا کرد.

بهر حال زمانیکه مجموعه وسیعی از اطلاعات را با هر روش ممکن ذخیره نمائیم، می بایست روشهائی را نیز برای بازیابی و دستیابی به آنان تدوین نمود. در مدلهای قدیمی جهت حرکت از یک صفحه (یک حریم اطلاعاتی) به صفحه دیگر، می بایست بصورت خطی حرکت نمود.(ابتدا صفحه یک و در ادامه صفحه دو و ...) در یک ابر متن با استفاده از اطلاعات تعریف شده میتوان از یک واژه به واژه دیگر پرش و اطلاعات مربوطه را مشاهده نمود.مثلا" در یک دایره المعارف که بصورت ابر متنی پیاده سازی شده است، میتوان اطلاعاتی را در رابطه با " نیما یوشیج " مشاهده و در همان وضعیت اطلاعاتی را نیز در رابطه با " یوشیج " زادگاه وی مشاهده نمود. در زمان مشاهده اطلاعات در رابطه با "یوشیج " میتوان اطلاعاتی را در رابطه با استان مازندران نیز دریافت کرد. در گذشته اکثر اطلاعاتی که از طریق وب دراختیار استفاده کنندگان قرار می گرفت بصورت"متن"(Text) بود، ولی امروزه با بکارگیری امکانات چند رسانه ای (MultiMedia) نظیر صوت، گرافیک، انیمیشن و تصویر میتوان اطلاعات را با اشکال متفاوت بر روی سایت های اطلاعاتی مشاهده نمود. مثلا" میتوان یک سایت اطلاعاتی از فیلم های ویدئوئی را ایجاد و علاقه مندان به استفاده از سایت، از طریق وب قادر به دستیابی فیلم مورد علاقه خود خواهند بود.

وب بعنوان بخشی از اینترنت محسوب میگردد (اینترنت یک شبکه گسترده جهانی از کامپیوترهای بهم مرتبط می باشد). وب یک سیستم مدیریت بانک اطلاعاتی سرویس دهنده / سرویس گیرنده بوده که از یک ساختار و معماری مشخص جهت بازیابی اطلاعات استفاده می کند. تمامی مرورگرها (Browser) با آگاهی از این معماری قادر به دستیابی به اطلاعات موجود خواهند بود. مرورگرها، نرم افزارهائی هستند که پس از نصب و بهره برداری از آنان میتوان از یک سایت اطلاعاتی به سایت دگر حرکت نمود.اولین بار یک برنامه نویس انگلیسی بنام " برنرز لی " ایده ترکیب ابر رسانه ها را منابع اطلاعاتی اینترنت مطرح نمود. قبل از وب منابع و اقلام اطلاعاتی گوناگونی در

اینترنت وجود داشت ولی دستیابی به آنها بسادگی میسر نبود. در سال ۱۹۸۹"زمانیکه" برنرزلی" بر روی یک پروژه فعالیت می کرد، مشاهده نمود که دستیابی به اطلاعات مورد نیاز جهت کار همزمان بر روی پروژه برای افراد، عملیاتی طاقت فرسا و مشکل است.وی با بهره گیری از تکنولوژی ابر متن ها، شبکه ای از مستندات مورد نیاز افراد جهت فعالیت در پروژه های گوناگون را فراهم آورد. در این حالت ارتباطات متعددی به صفحات مستندات، ایجاد و تمامی جزئیات مربوطه از دید استفاده کننده مخفی می ماند.

مستندات وب ، می بایست با یک قالب خاص نوشته شوند، بگونه ای که ابر متن ها بتوانند با یکدیگر کار نمایند. این قالب خاص HTML Hyper Text Markup Language)) نامیده شد.

این زبان بعنوان زیر مجموعه زبان (SGML Standard Generalized Markup Language) محسوب میگردد.SGML استانداردی جهت تعریف فورمت در مستندات متنی است.از استاندارد فوق در گذشته اغلب جهت عملیات مربوط به نشر رومیزی استفاده می شد." برنرزلی " از قابلیت های ابرمتن ها برای ایجاد اولین مستندات در وب استفاده نمود.جهت دستیابی به اولین سایت های وب از یک مرورگر خطی وب استفاده می شد. این مرورگر محدود به استفاده از صرفا" یک خط از اطلاعات بود. در این مدل می بایست از یکی از نرم افزارهای اینترنت بنام TelNet جهت دستیابی به دو سایت اولیه وب با نامهای Infacern.ch و یا Nxo01.cern.ch استفاده میگردید. این مرورگر دارای دستوراتی نظیر: Start a Search و Follow a Link بود. اکثر اطلاعات موجود در سایت های اولیه ، از امکانات ابر متن ها استفاده نمی کردند و همین امر باعث عدم بکارگیری قابلیت های ابرمتن ها در مستندات اولیه و عدم رشد مناسب وب گردید. مهمترین عامل رشد و فراگیر شدن وب در سطح جهان، عرضه مرورگر " موزائیک " به بازار بود.

موزائیک (تولد نسل جدیدی از مرورگرها)

" مارک آندرسون " در سال ۱۹۹۳ پروژه تولید و طراحی نرم افزار موزائیک را هدایت نمود. هدف از طراحی موزائیک، ارائه راهکاری مناسب برای افرادی بود که بر روی پروژه های متفاوت فعالیت داشته و ملزم به استفاده و دستیابی به اطلاعات مشترک بودند.در ابتدا " آندرسون " از وجود وب هیچگونه اطلاعی نداشت و جهت ارائه راه حل مناسب، تحقیقات گسترده ای توسط وی انجام و در نهایت وی وب را بعنوان یک را ه حل مناسب کشف نمود. پس از شناخت پتانسیل های وب توسط " آندرسون "، ایده طراحی موزائیک بعنوان مرورگر وب توسط وی مطرح گردید.در آوریل ۱۹۹۳ اولین نسخه موزائیک (Ver 1.0) برای سیستم Windows ارائه گردید.این برنامه بسرعت در سطح جهان مطرح و باعث اعتبار و شهرت فراوان وب گردید. بدلیل اعتبار و عمومیت یافتن موزائیک، NCSA (مرکز ملی برنامه های فوق محاسباتی) نسخه های ویندوز و اپل مرورگر فوق را پیاده سازی نمود. مرکز فوق با توجه به تعریف خاص حوزه فعالیت خود مجبور به فروش امتیاز " موزائیک " به چندین شرکت از جمله: Mosaic Communication و Quarterdeck spry شد.در سال ۱۹۹٤ " مارک آندرسون "NCSA را ترک و به یک شرکت جدیدالتاسیس بنام " نت اسکیپ" (NetScape) پیوست. پس از پیوستن وی به نت اسکیپ، مرورگر جدیدی توسط این شرکت طراحی وبا نام Netscape Navigator به بازار عرضه گردید. این مرورگر انقلابی در زمینه مرورگرها را بوجود آورد و پس از مدت زمان کوتاهی بعنوان پرفروشترین مرورگر در سطح جهان مطرح گردید.

رشد و توسعه وب

وب با یک سرعت حیرت انگیز در حال رشد و توسعه است.امروزه در اکثر برنامه های تلویزیونی و پخش آگهی های تجاری کمترین آگهی را میتوان مشاهده نمود که متقاضیان

را جهت کسب اطلاعات بیشتر به یک وب سایت هدایت ننماید. یک وب سایت، سیستمی بر روی اینترنت است که شامل سرویس دهنده وب (Web Server) است. این سرویس دهنده ، نرم افزاری بر روی سایت است که امکان دستیابی مرورگرهای وب را به مستندات موجود فراهم می کند.در گذشته بدلیل ترافیک بالای مصارف سیاسی از اینترنت، زمینه استفاده از آن در بعد تجاری و اقتصادی فراهم نبود.در سال ۱۹۹۱ با پیدایش ایده تبادل اقتصادی اینترنت CIX (Commerical Internet Exchange) وضعیت فوق تغییر کرد. CIX توسط ارائه دهندگان سرویسهای اینترنت تحت AlterNet,CERfent,PSInet ارائه گردید. این سیستم با موفقیت و استقبال چشمگیری مواجه گردید.امروزه اغلب تولید کنندگان کالا در سطح جهان اطلاعات مربوط به کالای خود را بر روی وب و از طریق سایت های شناخته شده ای ارائه میدهند.متقاضیان کالا در هر نقطه از جهان با مراجعه به سایت مربوط به آن شرکت و یا شرکت های مشابه میتوانند آگاهانه نسبت به انتخاب کالای مورد علاقه خود اقدام و از طریق وب، فرآیند ثبت سفارش را انجام دهند.برخی دیگر از شرکت ها در سطح جهان بالاخص شرکت های کامپیوتری سرویس های فنی و پشتیبانی خود را به مشتریان از طریق وب انجام میدهند. مثلا" با مراجعه به سایت ماکروسافت علاوه بر امکان خرید محصول مورد نظرخود، درصورتیکه در زمینه بکارگیری یکی از محصولات نرم افزاری آن شرکت دارای سوالات و ابهاماتی باشیم، با استقرار در بخش فنی و پشتیبانی میتوان پاسخ و رهنمودهای لازم را دریافت کرد.برخی دیگر از شرکت ها بالاخص شرکت های انتشاراتی و چاپ مجلات، روزنامه ها، اطلاعات خود را (روزنامه ها و مجلات) بر روی شبکه قرارداده و زمینه استفاده و یا خرید را برای متقاضیان فراهم می نمایند. تمامی متقاضیان جهت خرید کالای مورد نیاز خود از طریق وب، می بایست دارای یکی از انواع متداول کارتهای اعتباری نظیر : Credit Card و یا MasterCard باشند.

پس از انتخاب کالا از طریق متقاضی و تعیین نحوه پرداخت شماره مربوط به کارت اعتباری می بایست به سیستم داده شود. ثبت و درج شماره کارتهای اعتباری یکی از مسائل مهم در زمینه امنیت در تجارت بر روی اینترنت است. هر فرد می بایست این اطمینان را داشته باشد که از شماره کارت اعتباری وی استفاده غیر قانونی بعمل نمی آید. به همین دلیل وب مجهز به یک سیستم رمزگذاری مطمئن جهت کارت های اعتباری است.

اصول و تعاریف اولیه در رابطه با وب

اطلاعات موجود در وب در حریم های اطلاعـــــــاتی با نام " صفحات وب " ذخیـــره می گردنند. اندازه ونوع محتویات این نوع صفحات کاملا" متغیر بوده و نمی بایست در این راستا یک صفحه وب را با یک صفحه کتاب مقایسه کرد گرچه شباهت های اندکی نیز بین آنها وجود داشته باشد.

محتویات یک صفحه وب می تواند: متن رافیک صدا تصویر انیمیشن و ... باشد. گستردگی و تنوع نوع اطلاعاتی که می توان در صفحات وب قرار داد یکی از مهمترین ویژگی های قابل توجه وب از دیدگاه ارائه دهندگان اطلاعات از یکطرف و استفاده کنندگان از اطلاعات از طرف دیگر می باشد.

صفحات وب از لحاظ فیزیکی فایل های هستند که توسط نرم افزارهای مربوطه بوجود آمده و دارای انشعاب "htm" و یا "html"" می باشند. برای ایجاد این نوع صفحات می توان از تمام نرم افزارهائی که بنوعی قادر به ایجاد و ذخیره سازی یک فایل هستند استفاده کرد.(Notepad نمونه ای از این نوع نرم افزارها است). امروزه نرم افزارهای کاملا" حرفه ای برای ایجاد و مدیریت صفحات وب توسط شرکت های

نرم افزاری ایجاد شده است . FrontPage,Hotmetal،... نمونه هائی در این زمینه می باشند.پس از ایجاد صفحات وب در صورت نیاز و استفاده عموم (داخلی ، خارجی) می بایست آنها را بر روی یک سایت ذخیره نمود. یک وب سایت مجموعه ای از صفحات وب را شامل می گردد.

ارائه دهندگان اطلاعات پس از آماده سازی صفحات وب و استقرار آنها بر روی یک وب سایت زمینه استفاده از اطلاعات فوق را برای استفاده کنندگان فراهم می نمایند. استفاده کنندگان با استفاده از نرم افزارهائی موسوم به " مرورگر" قادر به دستیابی به یک وب سایت و درخواست اطلاعات مورد نیاز خود می باشند.

تمام صفحات وب دارای مجموعه دستورالعمل هائی هستند که نحوه نمایش اطلاعات مورد نظر را مشخص خواهد کرد. رایج ترین مجموعه دستورالعمل های نمایش در صفحات وب تگ های Html می باشند.

همانطور که اشاره گردید برای ایجاد مجموعه دستورالعمل های نمایش در صفحات وب از شبه زبان Html استفاده می گردد.شبه زبان فوق، را نمی توان بعنوان یک زبان برنامه نویسی در نظر گرفت چراکه عملا" دستورالعمل های پردازش را شامل نشده و صرفا" در حد توصیف نحوه نمایش محتویات است. Html دارای مجموعه ای از کدهای توصیفی برای نمایش اطلاعات در مرورگرها است. این زبان دارای مجموعه ای از تگ ها است که هر یک دارای معانی و عملکرد از قبل مشخص شده هستند. مثلا" تگ :<B> برای پررنگ نمودن متن مورد نظر و یا تگ
 برای ایجاد یک خط خالی استفاده می شود. فایل هائی که بکمک Html ایجاد می گردنند می بایست دارای انشعاب "Html" و یا "Htm" باشند. در حقیقت تگ های Html سیاست های مربوط به نحوه نمایش اطلاعات در مرورگرهای وب را مشخص و مرورگرهای وب پس از تفسیر

تگ های استفاده شده واکنش های از قبل تعریف شده را از خود نشان خواهند داد.
بنابراین می توان Html را بعنوان زبانی برای تبین نحوه نمایش اطلاعات تعریف کرد.

مثال : یک نمونه فایل HTML

```
<html>
                                        <head>
                  <title>صفحه      عنوان      </title>
                                        </head>
<body>
                  <                 .....          >
</body>
</html>
```

html دارای نسخه های متعددی از بدو پیدایش تاکنون بوده است. در زمان ایجاد یک صفحه وب می بایست، نوع نسخه استفاده شده Html را مشخص نمود. این عملیات توسط DOCTYPE انجام می گیرد. هر یک از نسخه های فوق دارای مجموعه تگ های مربوط به خود خواهند بود. در ادامه به انواع این نسخه ها و نحوه تعریف کردن و مشخص نمودن نوع نسخه در صفحات وب اشاره می گردد.

HTML 2.0 نسخه فوق بعنوان استاندارد اولیه (RFC 1866) معرفی گردید.

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML Strict//EN">
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML//EN">
```

Html 3.2 استاندارد معرفی شده توسط کنسرسیوم وب است.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
```

Html 4.0 استاندارد معرفی شده توسط کنسرسیوم وب که دارای سه گرایش متفاوت است:

- ***Strict HTML 4.0*** . این نسخه امکان استفاده از فریم و اغلب ویژگی هائی نظیر ″ تراز بندی ″ را شامل نمی شود.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0//EN"
  "http://www.w3.org/TR/REC-html40/strict.dtd">
```

- ***Transitional HTML 4.0*** امکانات مربوط به نمایش نظیر ″ ترازبندی ″ را دارا بوده ولی همچنان امکان استفاده از فریم ها وجود نخواهد داشت.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0
Transitional//EN"
  "http://www.w3.org/TR/REC-html40/loose.dtd">
```

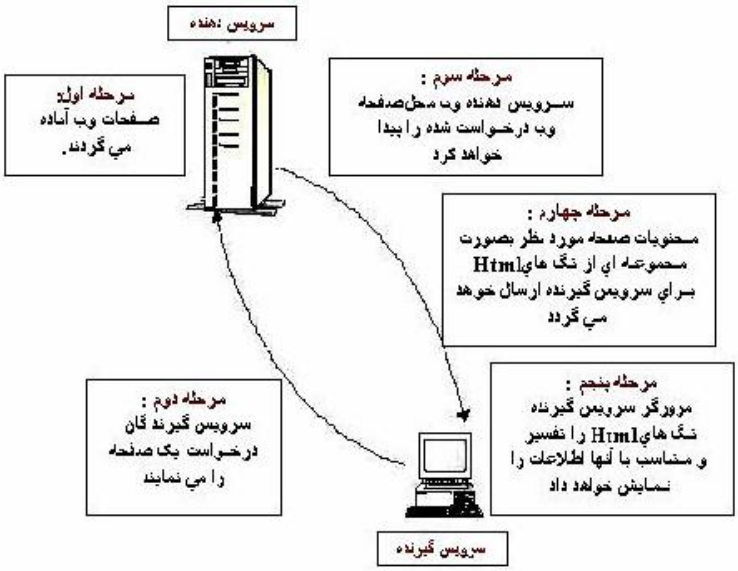
- ***HTML 4.0 Frameset*** . امکان استفاده از فریم را دارا است.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0
 Frameset//EN"
  "http://www.w3.org/TR/REC-html40/frameset.dtd">
```

محدودیت های Html

اطلاعات موجود در وب در حریم های اطلاعاتی با نام ″صفحات وب″ ذخیره می گردنند. اندازه ونوع محتویات این نوع صفحات کاملا″ متغیر بوده و نمی بایست در این راستا یک صفحه وب را با یک صفحه کتاب مقایسه کرد گرچه شباهت های اندکی نیز بین آنها وجود داشته باشد.

صفحات وب ایستا ، امروزه بر روی اینترنت و وب، با سایت های متعددی که شامل تعداد بیشماری از صفحات وب ایستا می باشند، برخورد می نمائیم. واژه " **ایستا** "، در رابطه با یک صفحه وب دارای چه تعریفی است؟ این نوع صفحات، صفحاتی هستند که شامل کدهای Html بوده و در یک محیط ادیتور تایپ و با انشعاب Htm و یا Html ذخیره می گردد. مولف صفحه وب قبل از اینکه هر نوع درخواستی برای آن وجود داشته باشد، بطور کامل محتوی صفحه را مشخص کرده است. محتویات این نوع از صفحات (متن، تصویر، لینک ها و...) و شکل ظاهری آنها **همواره یکسان** خواهد بود، صرفنظر از اینکه **چه کسی**، در **چه زمانی** و یا **چگونه** صفحه را مشاهده خواهد کرد. بنابراین می توان گفت، محتویات این قبیل از صفحات قبل از اینکه درخواستی ایجاد گردد ، توسط مدیریت سایت ایجاد و مشخص شده اند.



مراحل آماده سازی صفحات وب ایستا

۱ – یک مولف صفحه ای را که شامل کدهای Html است را ایجاد و آن را با انشعاب Htm و یا Html بر روی سرویس دهنده وب ذخیره می نماید.

۲ – کاربری از طریق برنامه مرورگر خود، در خواست استفاده از یک صفحه را می نماید، درخواست فوق از مرورگر برای سرویس دهنده ارسال می گردد.

۳ – سرویس دهنده وب، فایل درخواستی با انشعاب Htm و یا Html را پیدا خواهد کرد.

٤ – سرویس دهنده وب، کدهای Html فایل مزبور را از طریق شبکه برای مرورگر ارسال میدارد.

٥ – مرورگر کدهای Html را پردازش و صفحه فوق را نمایش خواهد داد.

محدودیت های صفحات وب ایستا

فرض کنید می خواهیم یک صفحه وب را بگونه ای طراحی نمائیم، که بمحض ورود هر کاربر زمان جاری سیستم بهراه یک پیام مناسب نمایش داده شود.. در این زمینه با چندین محدودیت مواجه خواهیم بود که بکمک تگ های Html قادر به برطرف کردن آنها نخواهیم بود. ما میدانیم که یک کاربر در یک زمان خاص به ملاقات صفحه خواهد آمد ولی قطعا؛ زمان آن را نمی دانیم .اگر بخواهیم زمان را بصورت کد در صفحه Html خود داشته باشیم ، نتیجه همواره یکسان بوده و همیشه یک زمان ثابت و یکسان برای تمامی ملاقات کنندگان صفحه، نمایش داده خواهد شد. تگ های Html امکاناتی بمنظور ایجاد صفحات وب سفارشی و بر اساس شرایط خاص در اختیار قرار نمی دهد. صفحات وب ایستا همواره بصورت مشابه و یکسان برای تمامی کاربران نمایش داده خواهند شد. (نظیر رستورانی که همواره و صرفنظر از ذائقه مشتریان خود، یک غذای ثابت و از قبل آماده شده را برای همه آماده و در اختیار قرار می دهد!)

Html دارای هیچگونه امنیتی نیز نبوده و کدهای آن را همه می توانند مشاهده و حتی

تکثیر گردد. شاید تنها مزیت این نوع از صفحات طراحی آسان و بکارگیری سریع آنان در یک شبکه باشد. این نوع صفحات دارای امکانات لازم بمنظور آفرینش صفحات پویا نیستند، چون نمی توان کدهای مورد نظر خود را بعد از درخواست یک صفحه به آن اضافه کرد . می بایست بدنبال روشی و یا روش هائی بود که بکمک آنها بتوان صفحات وب پویا را ایجاد کرد. بمنظور نیل به هدف فوق از دو روش عمده استفاده می گردد:

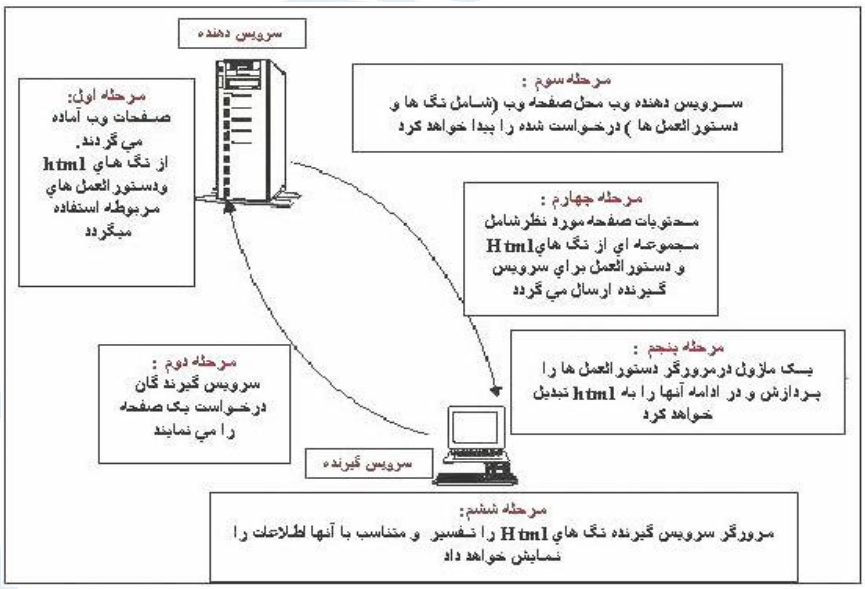
page Client - side dynamic . بهره گیری از تکنولوژیهائی که پویائی یک صفحه را از جایگاه سرویس گیرنده تحقق خواهند داد.

page side dynamic – Server . بهره گیری از تکنولوژیهائی که پویائی یک صفحه را از جایگاه سرویس دهنده تحقق نمایند.

قبل از پرداختن به هر یک از موارد فوق، لازم است در ابتدا با مفهوم و جایگاه یک سرویس دهنده وب بیشتر آشنا شویم . یک سرویس دهنده وب، نرم افزاری است که مدیریت صفحات وب را برعهده گرفته و آنها را برای سرویس گیرندگان مجهز به مرورگرها، قابل دستیابی و استفاده می نماید. تاکنون سرویس دهنده های وب متعددی طراحی و به بازار عرضه شده است. Apache ، IIS ... نمونه هائی از این نوع نرم افزارها هستند. IIS محصول شرکت مایکروسافت بوده و می توان در زمان نصب ویندوز (۲۰۰۰ و یا XP) آن را نیز نصب نمود.نسخه ۵ بهمراه ویندوز ۲۰۰۰ و نسخه ۵،۱ بهمراه XP ارائه شده است . بهرحال جایگاه یک سرویس دهنده وب در ارائه امکانات و زیرساخت های مناسب برای طراحی صفحات وب پویا و بالطبع سایت های پویا یک امر برجسته است. همانگونه که اشاره گردید، برای خلق صفحات وب پویا از دو رویکرد متفاوت استفاده می گردد. استفاده همزمان از دو روش فوق هیچگونه تعارضی با هم

نداشته بلکه بالعکس توانائی یک صفحه وب پویا را افزایش خواهد داد. درادامه به بررسی دو رویکرد فوق خواهیم پرداخت.

page Client-side dynamic . در مدل فوق ماژول هائی (Plug –in) که به مرورگر ملحق شده اند، تمامی عملیات لازم جهت ایجاد صفحات پویا را انجام خواهند داد. کدهای Html از طریق فایل مربوطه که شامل مجموعه ای از دستورالعمل ها است برای مرورگر ارسال خواهد شد.مرورگرها دستورات فوق را جهت تولید کدهای Html و در زمان درخواست یک صفحه توسط کاربر، استفاده خواهند کرد. بنابراین محتویات یک صفحه بر اساس درخواست کاربران و بصورت پویا ایجاد خواهد شد.



مراحل آماده شدن یک صفحه وب پویا با تاکید بر روش های Client-Side

۱ – یک مولف صفحه وب مجموعه ای از دستورالعمل را برای ایجاد کدهای Html نوشته و آنها را در فایلی با انشعاب Html ذخیره می نماید.

۲ – کاربران درخواست یک صفحه را از طریق مرورگر خود برای سرویس دهنده وب ارسال خواهند کرد.

۳ – سرویس دهنده فایل درخواستی (در صورت نیاز فایل دیگری که شامل دستورالعمل ها باشد) را پیدا خواهد کرد.

٤ – سرویس دهنده وب فایل حاوی کدهای Html و در صورت وجود دستورالعمل های مربوطه را برای متقاضی ارسال خواهد کرد.

٥ – یک ماژول همراه مرورگر ، دستورالعمل ها را پردازش و کدهای Html را در همان صفحه Html برمی گرداند.

٦ – در نهایت کدهای Html توسط مرورگر نمایش داده می شوند.

تاکنون تکنولوژیهای متعددی بر اساس رویکرد فوق مطرح و در اختیار طراحان و مولفان صفحات وب پویا قرار گرفته شده است. جاوا اسکریپت، Vbscript، کنترل های ActiveX و اپلت های جاوا نمونه هائی از این نوع تکنولوژی ها بوده که برای شناخت خوانندگان در این بخش بصورت خیلی مختصر در رابطه با هر یک توضیحاتی ارائه خواهد شد.

جاوااسکریپت (JavaScript) ،اولین زبان اسکریپت در رابطه با مرورگرها است. زبانهای اسکریپت بعنوان حد میانه بین کدهای Html و زبانهای معمولی برنامه نویسی قرار داشته و بصورت مفسر عمل می نمایند. جاوااسکریپت را نباید با زبان برنامه نویسی جاوا اشتباه گرفت. شرکت نت اسکیپ در ابتدا زبان اسکریپتی با نام LiveScript پیاده سازی و بهمراه مرورگر NetScape 2.0 در اختیار علاقه مندان قرار گرفت. زمانیکه

شرکت نت اسکیپ با شرکت Sun متحد گردید، نام آن را جاوااسکریپت گذاشتند. بخشی از گرامر زبان فوق نظیر ساختار اولیه، از جاوا گرفته شده است (خود جاوا نیز اغلب ساختار خود را از زبان C گرفته است). جاوااسکریپت دارای امکانات متعدد و قدرتمندی جهت کنترل و مدیریت رفتار و محتویات یک مرورگر است. زبان فوق توانائی انجام عملیاتی نظیر : عملیات روی فایل ها را دارا نمی باشد. (شاید یکی از دلایل مسائل امنیتی باشد). فراگیری جاوااسکریپت نسبت به جاوا بمراتب راحت تر است. جاوا اسکریپت بگونه ای طراحی شده است که قادر به خلق برنامه های کوچک و در عین حال موثر جهت انجام عملیات متعددی نظیر برخورد با رویدادهای بوجود آمده در سطح کاربر نظیر: کلیک نمودن بر روی یک آیتم، بستن یک پنجره، فعال شدن یک صفحه، خارج شدن از یک صفحه، حرکت موس روی یک آیتم و...است. ماکروسافت نسخه اختصاصی خود از جاوااسکریپت را با نام Jscript و همزمان با معرفی مرورگر IE 3.0 در اختیار علاقه مندان قرار داد.

Vbscript . شرکت ماکروسافت همزمان با عرضه مرورگر IE 3.0 زبان اسکریپت اختصاصی خود یعنی Vbscript را مطرح نمود. زبان اسکریپت فوق بر اساس زبان برنامه نویسی ویژوال بیسیک و با هدف رقابت با جاوااسکریپت در اختیار علاقه مندان قرار گرفت . شاید از معدود امتیازات این زبان نسبت به جاواسکریپت بتوان به عدم حساسیت آن در رابطه با حروف بزرگ و کوچک (Case Sensitive) نام برد. کدهای نوشته شده توسط زبان فوق صرفا؛ از طریق مرورگر شرکت ماکروسافت (IE) قابل تفسیر و اجرا بوده و نت اسکیپ این زبان را حمایت نمی کند، گرچه با افزودن برخی Plug-In امکان استفاده از این زبان در مرورگر نت اسکیپ نیز فراهم خواهد شد. استفاده از زبان جاوااسکریپت بمراتب نسبت به زبان Vbscript رایج تر است. اگر قصد انتخاب یک زبان اسکریپت برای پردازش های متکی بر سرویس گیرنده را داشته باشیم،

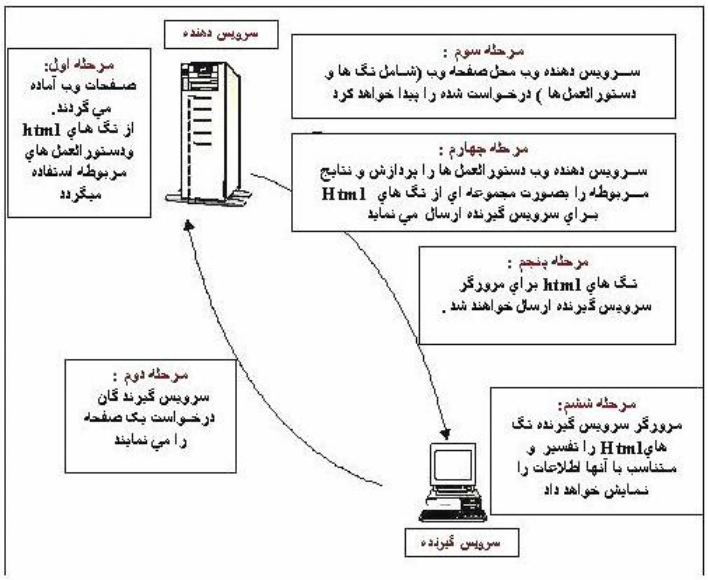
بدون شک جاواسکریپت یک گزینه مناسب خواهد بود. جاواسکریپت و Vbscript هر دو بعنوان یک ماژول با نام Script Engine که بهمراه مرورگرها ارائه شده است، مسئولیت تفسیر و اجرای دستورالعمل های مربوطه را بر عهده خواهند گرفت. در پروژه دات نت شرکت ماکروسافت VB.NET را جایگزین Vbscript نموده است.

کنترل های ActiveX ، یک کنترل اکتیوایکس عنصری است که توسط یکی از زبانهای برنامه نویسی نظیر C++ و یا جاوا پیاده سازی می گردند. در زمانیکه این نوع اکتیوایکس ها را بهمراه صفحات خود استفاده نمائیم، امکان انجام بخشی از عملیات متکی بر سرویس گیرنده نظیر ایجاد یک Bar Chart ، Timer ، تایید کاربر و یا دستیابی به بانک اطلاعاتی فراهم می گردد. کنترل های اکتیوایکس از طریق تگ <Object> به صفحات وب اضافه خواهند گردید. منادی تکنولوژی فوق شرکت ماکروسافت بوده و تا نسخه شش مرورگر نت اسکیپ امکان استفاده از آنها توسط مرورگر فوق وجود ندارد. البته با نصب برخی Plug-in زمینه استفاده از کنترل های اکتیوایکس در مرورگر نت اسکیپ بگونه ای فراهم شده است. نکته جالب توجه در رابطه با تکنولوژی فوق این است که امکان انجام عملیات متفاوت بر روی کامپیوترهای کاربران نظیر کار با فایل ها و ریجستری ویندوز بوجود می آید و این خود می تواند از لحاظ امنیتی مشکل و گاها " با توجه به وجود فایروال ها تحقق نا پذیر باشد. بهرحال نمی توان بر روی تکنولوژی فوق بعنوان یک راه حل جامع و فراگیر برای خلق صفحات وب پویا استفاده کرد مگر اینکه مخاطبان سایت خود را صرفا" از بین کسانی انتخاب نمائیم که ویندوز را بعنوان سیستم عامل و مرورگر IE را بعنوان مرورگر خود برگزیده اند.

Java Applet ، جاوا یک زبان برنامه نویسی مستقل از Platform است. جاوا نسبت به زبانهای اسکریپت دارای قابلیت های بمراتب بیشتری است. هدف، استفاده از کدهای جاوا به شکل اپلت است . عناصر فوق بسادگی و توسط تگ <Applet> به صفحات

وب ملحق خواهند شد. خوشبختانه مرورگرهای ماکروسافت و نت اسکیپ هر دو از طریق ایجاد یک ماشین مجازی جاوا (JVM) از اپلت های جاوا حمایت می کنند. بمنظور استفاده از اپلت های جاوا در یک صفحه وب از چندین روش می توان استفاده کرد: استفاده از تگ استاندارد <Object> یا استفاده از تگ غیراستاندارد <Applet> . تگ های فوق به مرورگر خواهند گفت که یک فایل جاوا را از طریق سرویس دهنده وب DownLoad و سپس بکمک ماشین مجازی جاوا (JVM) ، موجود در مرورگرها، آن را اجراء نماید. همانطور که حدس زده اید یکی از مسائل موجود در رابطه با استفاده از اپلت ها جاوا ، زمان اضافه ای است که صرف Download کردن، می گردد. بنابراین در زمان استفاده از اپلت های جاوا ، سعی در نوشتن اپلت ها با کد کم باشیم. از رایج ترین موارد کاربرد اپلت های جاوا می توان به ایجاد Drop-Down Menu و انیمیشن های متفاوت اشاره کرد.

Pages Server Side Dynamic . در این مدل کدهای Html بهمراه مجموعه ای از دستورالعمل ها برای سرویس دهنده ارسال و مجددا" از دستورالعمل های فوق برای تولید کدهای Html برای صفحه ای که کاربر درخواست کرده، استفاده شده و در نهایت صفحه بصورت پویا بر اساس درخواست کاربر ایجاد خواهد شد.



مراحل آماده شدن یک صفحه وب پویا با تاکید بر روش های Server-Side

۱ – یک مولف صفحه وب ، مجموعه ای از دستورالعمل ها را برای ایجاد کدهای Html نوشته و دستورالعمل ها را در یک فایل ذخیره می کند.

۲ – کاربران از طریق مرورگر خود، درخواست یک صفحه وب را نموده و این درخواست برای سرویس دهنده وب ارسال خواهد شد.

۳ – سرویس دهنده وب محل فایل حاوی دستورالعمل را پیدا خواهد کرد.

٤ – سرویس دهنده وب دستورات موجود در فایل را بمنظور تولید کد Html اجراء خواهد کرد.

۵ – سرویس دهنده وب کدهای تولید شده جدید را از طریق شبکه برای مرورگر ارسال می نماید.

٦ – مرورگر کدهای Html را پردازش و در نهایت صفحه وب نمایش داده خواهد شد.

یکته مهم در سناریوی فوق، **اجرای تمامی پردازش ها بر روی سرویس دهنده**، قبل از ارسال صفحه برای مرورگر است. یکی از مزایای عمده مدل فوق نسبت به مدل Client-Side ، این مورد است که : در یک صفحه وب صرفا" شاهد کدهای Html خواهیم بود. این بدان معنی است که منطق صفحات وب در نزد سرویس دهنده وب مخفی نگهداری خواهد شد و می توان این اطمینان را داشت که اکثر مرورگرها قادر به نمایش نتایج پردازش ها ی اجراء شده بر روی سرویس دهنده باشند. ASP.NET از مدل فوق تبعیت می کند. یکی دیگر از نکات مهم در رابطه با مدل فوق، این است که یک صفحه تا زمانیکه درخواستی برای آن دریافت نشده باشد، محتویات آن بوجود نخواهد آمد. در ادامه به بررسی برخی تکنولوژیهای متداول دراین مدل خواهیم پرداخت.

CGI(Common Gateway Interface) . مکانیزمی برای ایجاد اسکریپت بر روی سرویس دهنده بوده تا بدین طریق امکان ایجاد برنامه ها ی متکی بر وب فراهم گردد. CGI ماژولی است که می بایست به سرویس دهنده وب اضافه گردد. قدمت استفاده از تکنولوژی فوق بمراتب بیشتر از ASP است و تا کنون تعداد بیشماری از صفحات وب پویا با استفاده از تکنولوژی فوق و بکمک یک زبان اسکریپت ایجاد شده اند. CGI این امکان را فراهم خواهد کرد که کاربر، یک برنامه دیگر (نظیر یک اسکریپت Perl) را بر روی سرویس دهنده برای ایجاد صفحات وب پویا استفاده نماید. استفاده از زبانهائی نظیر C++, C , Perl بهمراه تکنولوژی فوق بسیار رایج است. بهرحال تکنولوژی فوق امروزه در خیلی از سایت های بزرگ خصوصا" سایت های متکی بر یونیکس رایج بوده و قابلیت اجراء بر روی چندین Platform را دارا می باشند.

ASP(Active Server Page) ، تکنولوژی فوق که پس از عرضه ASP.NET با نام ASP کلاسیک نامیده می شود، یکی از متدوالترین روش هاب موجود و استفاده شده برای ایجاد صفحات وب پویا است. تکنولوژی فوق با بهره گیری از توان زبانهای اسکریپت نظیر جاوااسکریپت و Vbscript توانسته است پاسخ شایسته به طراح صفحات وب پویا را ارائه نماید. ASP یک ماژول جداگانه است که در کنار سرویس دهنده وب قرار می گیرد(ASP.dll) . تکنولوژی فوق نسبت به برخود از تکنولوژیهای همگروه از کارآیی پایین تری برخوردار بوده و در زمینه استفاده از زبانهاب اسکریپت در کنار خود، نیز دارای محدودیت است. بهرحال تکنولوژی فوق با سابقه شش ساله تاکنون توانسته است به خیل عظیم درخواست ها براب ایجاد صفحات پویا درست پاسخ دهد، ولی با ظهور خواسته ها و انتظارات جدید به چالش جدی کشیده شده است و شاید ظهور و تولد ASP.NET دلیل و پاسخی به برخی از انتقادات مطروحه در این زمینه باشد.

JSP (JavaServer page) ، تکنولوژی فوق امکان ترکیب Html ویا Xml را با کدهای جاوا فراهم می نماید. این فناوری برخلاف ASP که صرفا" توسط سرویس دهنده وب ماکروسافت (IIS) حمایت می گردد، توسط سرویس دهندگان متعددی حمایت شده است. JSP در مقایسه با ASP بمراتب دارای قدرت و سرعت بیشتری بوده و برنامه نویسان جاوا بخوبی با قابلیت های متعدد آن آشنائی دارند. JSP این امکان را فراهم می کند که برنامه های جاوا از ویژگی محیط های متکی بر Java2 نظیر JavaBeans و Java2 Libraries بخوبی استفاده نمایند.

ColdFusion . با استفاده از تکنولوژی فوق، امکان ساخت صفحات وب پویا فراهم می گردد. این تکنولوژی بصورت یک ماژول جداگانه است که می بایست بر روی سرویس دهنده وب نصب گردد. صفحاتی که توسط تکنولوژی فوق بوجود می آیند، توسط هر نوع مرورگری قابل خواندن و نمایش خواهند بود.

تکنولوژی فوق از مجموعه زیادی تگ که توسط نرم افزار ColdFusion ارائه شده است، استفاده می کند. نرم افزار فوق بر روی سرویس دهندگان متعددی حتی IIS نصب و قابل استفاده است. مهمترین مسئله در رابطه با تکنولوژی فوق در این است که از تگ های Html-Like استفاده می گردد (در ASP.NET از زبانهای برنامه نویسی و اشیاء استفاده می گردد). یکی دیگر از نکات مهم در رابطه با تکنولوژی فوق در این است که تهیه آن رایگان نبوده و می بایست بیش از هزار دلار برای تهیه آن هزینه نمود!

PHP ، تکنولوژی فوق که در ابتدا Personal Home Page نامیده می شد و اخیرا؛ PHP Hypertext Preprocessor نامیده می شود، یکی دیگر از تکنولوژیهای رایج برای ایجاد صفحات وب پویا است. تکنولوژی فوق بر خلاف ASP.NET . بصورت Cross-Platform بوده و بر روی اغلب سیستم ها نظیر ویندوز NT و اغلب نسخه های یونیکس قابل استفاده است. گرامر زبان فوق نظیر C و Perl است. تکنولوژی فوق دارای برخی از ویژگی های برنامه نویسی شی گراء بوده که امکان سازماندهی و کپسوله نمودن کدها را فراهم می آورد.

ASP.NET ، پس از معرفی تکنولوژیهای رایج در این گروه، زمینه مناسب برای آشنائی با تکنولوژی ASP.NET بوجود آمده است. ASP.NET نیز بعنوان یک ماژول بر روی سرویس دهنده قرار می گیرد (aspnetIsapi.dll). در کنار تکنولوژی فوق مجموعه عظیم دات نت قرار دارد. ASP کلاسیک دررابطه با استفاده از زبانهای اسکریپت محدود بوده و صرفا؛ به جاوااسکریپت و Vbscript ختم می گردد (Vbscript هم صرفا" توسط سیستم های متکی بر ویندوز قابل استفاده خواهد بود) ASP.NET. امکان استفاده از مجموعه وسیعی از زبانهای برنامه نویسی را فراهم

می کند. زبانهائی نظیر VB.NET ، C# ، Jscript.NET ، Python, Perl نمونه هائی از زبانهائی می باشند که می توان از آنها بهمراه ASP.NET استفاده کرد.

امروزه بیش از پانصد میلیون نفر در سراسر دنیا از اینترنت استفاده می نمایند. تعداد صفحات وب موجود در اینترنت از مرز چهار میلیارد گذشته و همچنان این روند با سرعتی باورنکردنی رو به افزایش است. حجم مبادلات تجاری بر روی اینترنت، از مرز نیم تریلیون دلار گذشته و افق جدیدی را برای تمامی بنگاه های تجاری در سرتاسر دنیا ایجاد نموده است. رشد و گسترش اینترنت در تمامی عرصه ها، تعجب اکثر کارشناسان و متخصصین را باعث شده است. به اعتقاد اغلب کارشناسان هنوز در میانه راه بوده و یک انقلاب دیجیتالی کامل و بسیار فراگیر را در آینده شاهد خواهیم بود.

وضعیت فعلی اینترنت در اغلب موارد، مشابه وضعیت مدل سیستم های بزرگ (Mainframe) در گذشته است. در قیاس فوق، مرورگرهای وب بمنزله ترمینال های سیستم های بزرگ بوده و دقیقا" در همان راستا ایفای وظیفه می نمایند. تمام اطلاعات موجود بر روی اینترنت در حال حاضر در بانک های اطلاعاتی متمرکز شده ای، ذخیره شده است . کاربران در هر لحظه قادر به دریافت **یک صفحه وب از یک وب سایت** می باشند. صفحات وب، صرفا" **تصویری از داده های مورد نیاز** کاربران بوده و داده های واقعی و اساسی را شامل نمی گردند. (شامل خود داده ها نمی باشند). اطلاعات موجود در صفحات وب را می توان دریافت کرد، ولی امکان ویرایش، تفسیر های جانبی و یا سایر عملیات مربوط به سفارشی نمودن داده ها، امری بسیار مشکل و در برخی حالات غیرممکن است. در صورتیکه برخی کاربران قصد استخراج و جمع آوری اطلاعات از چندین وب سایت را داشته باشند، می بایست در نهایت اطلاعات مورد نیاز را از صفحات وب متفاوت انتخاب و آنها را در یک فایل دیگر که با یک ادیتور خاص

نظیر notepad ایجاد شده است، قرار دهند. فرآیند فوق بصورت کاملا" دستی توسط کاربران انجام شده و عملا" یک حرکت سیستماتیک در این راستا انجام نمی گیرد. "تیم برنرز لی"، مبتکر وب، در زمان ایجاد وب بر خاصیت " محیط محاوره ای " آن تاکید فراوان داشت. وضعیت اشاره شده در رابطه با استخراج و جمع آوری اطلاعات مورد نیاز از وب سایت های متعدد، با ایده مطرح شده فوق فاصله زیادی دارد.

بمنظور گذر از وضعیت فعلی وب و ارتقاء آن به محیطی که صرفا" نمایش دهنده اطلاعات ایستا نباشد، لازم است نسل جدیدی از اینترنت که پاسخگوی نیاز ها و انتظارات فعلی و مشکلات موجود باشد، بوجود آید. وب سایت های موجود مشابه **جزایر اطلاعاتی** بوده که گرچه در هر یک از جزایر فوق ممکن است اطلاعاتی بصورت پویا نیز ایجاد گردد، ولی هیچگونه تعامل اطلاعاتی بین جزایر فوق وجود ندارد. تنها تعامل ارتباطی با جزایر فوق توسط کاربران آن سایت ایجاد می گردد. در این راستا لازم است ، کامپیوترها، دستگاههای هوشمند، سرویس های مبتنی بر وب در یک همیاری و همکاری تعریف شده، زمینه ارتباط و تعامل اطلاعاتی بین هر یک از جزایر اطلاعاتی را فراهم نمایند. در نسل قبلی اینترنت تمام تلاش در جهت بهبود نحوه ارتباط کاربران با هر یک از جزایر اطلاعاتی صرف گردید، در صورتیکه در نسل جدید اینترنت لازم است، تعامل اطلاعاتی بین جزایر اطلاعاتی بوجود آید و فصل جدیدی با نام " گفتمان برنامه های " موجود در هر یک از جزایر اطلاعاتی را شاهد باشیم، با حرکت بسمت مدل فوق، جزایر اطلاعاتی ایزوله شده از حالت محدود خود خارج شده و بین جزایر فوق ، پل های متفاوت اطلاعاتی ایجاد و عملا" با تحولی شگرف مواجه خواهیم شد. اغلب سرویس ها و امکانات ارائه شده به کاربران تاکنون از طریق همین جزایر اطلاعاتی ایزوله شده قرار می گرفت، در صورت ارتباط اطلاعاتی و تعریف شده بین جزایر اطلاعاتی، دستاوردهای بمراتب گسترده تری نسبت به وضعیت فعلی را بدنبال خواهد داشت.

XML(Language Extensible Markup)، هسته اساسی گذر از مرحله فعلی اینترنت و قدم گذاشتن در نسل جدید اینترنت است. XML ، یک استاندارد صنعتی ارائه شده توسط کنسرسیوم وب است که توسط اکثر شرکت های عظیم کامپیوتری در سطح دنیا پذیرفته شده و بعنوان محور توسعه در نسل جدید اینترنت مورد توجه و اهتمام جدی است. با استفاده از XML ، بین نحوه نمایش اطلاعات و خود اطلاعات ، یک تمایز و تفکیک ایجاد می گردد. XML در موارد متعدد، دارای عملکردی مشابه HTML است. در HTML با استفاده از تگ های موجود، نحوه نمایش اطلاعات در صفحات وب تعریف می گردد. در XML با استفاده از تگ های مورد نظر، ساختار مناسبی برای اطلاعات تعریف و امکان ارسال و استفاده از داده ها برای سرویس های دریافت کننده فراهم خواهد شد. XML ، امکان سازماندهی ، برنامه نویسی، ویرایش و مبادله اطلاعات با سایر سایت ها ، برنامه و دستگاهها را فراهم می آورد. بدین ترتیب هر یک از صفحات وب دارای یک بانک اطلاعاتی کوچک شده (اطلاعات مبتنی بر ساختارهای XML) که براحتی می توان با توجه به ساختار تعریف شده برای داده های موجود، از قابلیت های برنامه نویسی در جهت نیل به خواسته های مربوطه استفاده نمود. یک برنامه کامپیوتری با آگاهی از ساختار داده های ذخیره شده (ساختمان داده) قادر به انجام عملیات متفاوت و گوناگونی خواهد شد. مثلا" با دریافت اطلاعات مربوط به قیمت سهام از وب سایت مربوطه، می توان بر روی سایت خود انواع تحلیل های پویا و گزارشات مورد نظر را پس از انجام پردازش های لازم ، ارائه داد. پردازش های انجام شده در یک وب سایت بر روی داده ها(داده ها با استفاده از یک ساختار مناسب مبتنی بر XML تعریف می گردند) ممکن است با پردازش های انجام شده در وب سایت دیگر متفاوت باشد. در این راستا در ابتدا اطلاعات با استفاده از فایل های XML دریافت و پس از انجام پردازش های لازم و دلخواه، با فورمت مورد نظر (نه تحمیلی) در اختیار کاربران سایت قرار داده خواهد شد. XML در سناریوی فوق بمنزله پل اطلاعاتی بوده که اطلاعات را بر اساس

ساختار تعریف شده در اختیار سایر سایت ها (نمایندگان نرم افزاری مربوطه) قرار خواهد داد.

با استفاده از XML ، وب سایت های متعدد قادر به اشتراک و استفاده اطلاعات بین یکدیگر بوده و ضرورتی به استفاده از یک زبان برنامه نویسی و یا نرم افزاری خاص وجود نخواهد داشت. وب سایت ها با ایجاد سرویس های مبتنی بر وب، قادر به ایجاد یک ارتباط و تعامل هوشمندانه بین خود خواهند بود. بدین ترتیب اطلاعات بسادگی بین دستگاههای متفاوت حرکت خواهد کرد.

نسل جدید اینترنت یک پلات فورم ارتباطی و محاسباتی نظیر کامپیوترهای شخصی خواهد بود. برنامه هائی که برای اینترنت نوشته می گردند (نظیر برنامه هائی که برای کامپیوترهای شخصی نوشته می شود)، در وب سایت های متعدد قابلیت اجراء را داشته و پس از اخذ اطلاعات و خدمات از یکدیگر، با ترکیب و توزیع آنها با اشکال کاملا" خاص و سفارشی، امکان ارسال آنها برای هر دستگاه های مورد نیاز، فراهم خواهد شد. فاصله موجود بین اینترنت و کامپیوتر شخصی و یا سایر دستگاههای موجود حذف و نرم افزارهای پیشرفته ای بصورت اتوماتیک، اطلاعات مورد نیاز کاربران را بصورت محلی و یا از راه دور جمع آوری و در اختیار متقاضیان قرار خواهند داد.

در نسل جدید اینترنت فاصله موجود بین اطلاعات online ، سرویس ها و دستگاهها، شکسته (حذف) شده و انقلابی در زمینه نحوه ارتباط با آنها را شاهد خواهیم بود. امروزه، کاربران با استفاده و بکارگیری نرم افزارهای مجزا برای هر یک از عملیات مورد نظر خود، امکان اخذ اطلاعات ، نوشتن و یا ویرایش نامه های الکترونیکی و یا پیام های فوری و سایر موارد دلخواه را در اختیار دارند. در نسل جدید اینترنت، با رویکردی کاملا" مجتمع و همگن مواجه خواهیم بود. در این راستا، کاربران با استفاده از یک

اینترفیس (رابط) واحد، قادر به برقراری ارتباطی شفاف بین اینترنت و کامپیوتر شخصی و یا سایردستگاههای استفاده شده بوده و از این طریق امکان مشاهده، ویرایش، زمانبندی، ارتباط و آنالیز داده ها را پیدا خواهند کرد. کاربران قادربه برقراری ارتباط با سازمان متبوع خود بکمک روش های متعددی خواهند شد. امروزه تعداد نامه های الکترونیکی که هر فرد دریافت و حاوی نوشته های تایپ شده و یا حاشیه نویسی صوتی می باشند، بسیار محدود است. در آینده، اکثر پیام های اطلاعاتی با فورمتی بجز متن های تایپ شده در اختیار مخاطبان قرار خواهد گرفت.

بهرحال وضعیت اینترنت و وب بسرعت در حال تغییر است. برنامه های تحت وب دارای مسئولیتی بمراتب بیشتر نسبت به گذشته با توجه به سطح انتظارات و خواسته ها خواهند بود. تکنولوژی های متعدد در این زمینه تدوین، طراحی و عرضه شده است. XML ستاره ای بی فروغ در بین تمام تکنولوژی های ارائه شده بوده که بعنوان شاه کلید طلائی در این زمینه ایفای وظیفه می نماید. وب سایت های مبتنی بر HTML ، در آینده ای نه چندان دور به سایت های مبتنی بر XML تبدیل تا بتوانند در بین میلیون ها وب سایت موجود، **زبانی برای گفتن و گوشی برای شنیدن**، داشته باشند. بدین ترتیب وب سایت ها از حالت ایزوله و محدود و محصور در یک حصار فیزیکی و منطقی خارج و زمینه ارتباط اطلاعاتی بین آنها فراهم خواهد شد. کاربران اینترنت در این راستا بالاترین بهره را خواهند برد. آنان فقط خواسته خود را مطرح و با تمهیدات انجام شده، در سریعترین زمان ممکن، منطقی ترین و مبسوط ترین پاسخ به آنها ارائه خواهد شد. ، پاسخی که برای بدست آوردن آن، وب سایت های متعدد در تعامل اطلاعاتی با یکدیگر قرار گرفته تا بتوانند سطح جدیدی از انتظارات و خواسته ها را تحقق نمایند. نسل جدید اینترنت مستلزم وجود سایت هائی است که یاد گرفته اند چگونه با یکدیگر مراوده اطلاعاتی داشته و هر روز نیز بر این توان و پتانسیل نیز می افزایند.

تعاریف برنامه نویسی تحت وب

برای مشخص نمودن برنامه هائی با قابلیت اجراء بر روی وب، از واژه های متعددی استفاده می گردد : Web-enabled ، Web-based و Web application نمونه هائی در این زمینه می باشند. واژه های Web-Based و Web-enabled در برخی موارد بجای یکدیگر استفاده شده تا برنامه های نوشته شده برای اجراء بر روی وب، شبکه های مبتنی بر اینترنت نظیر اینترانت ها را تشریح و مشخص نمایند. به هر یک از برنامه های فوق ، می توان از طریق یک مرورگر دستیابی پیدا کرد. این نوع برنامه ها در موارد متعددی با یکدیگر متفاوت می باشند. طراحی برنامه های Web-Based (مبتنی بر وب)، بگونه ای است که قابلیت اجراء بر روی اینترنت و وب را داشته باشند، در مقابل برنامه های Web-enabled ، دارای یک اینترفیس مبتی بر وب بمنظور استفاده از قابلیت های نرم افرارهای موجود (نرم افزارهای سنتی) می باشند. نرم افزارهای فوق قبل از مطرح شدن وب ایجاد شده و با طراحی یک اینترفیس مبتنی بر وب می توان از امکانات آنها در صفحات وب نیز استفاده نمود. مثلا" می توان با طراحی یک فرم لازم، اطلاعاتی را از کاربران اخذ و با مراجعه به بانک های اطلاعاتی موجود، اطلاعات مورد نظر را استخراج و نتایج را با یک فرمت مناسب برای مرورگر ارسال کرد. بهرحال برنامه های مبتنی بر وب، از آغاز با رویکرد وب، طراحی و پیاده سازی شده در صورتیکه برنامه های Web-enabled ، از نرم افزارهای موجود بکمک یک اینترفیس مبتی بر وب استفاده می نمایند.

برنامه های Web-Based ، دارای امکانات و قابلیت های متعددی بوده که بمنظور استفاده در وب طراحی و پیاده سازی شده اند. برنامه های Web-enabled ، دارای یک Gateway مجزا تحت وب بوده که امکان ارتباط با نرم افزارهای قدیمی را فراهم

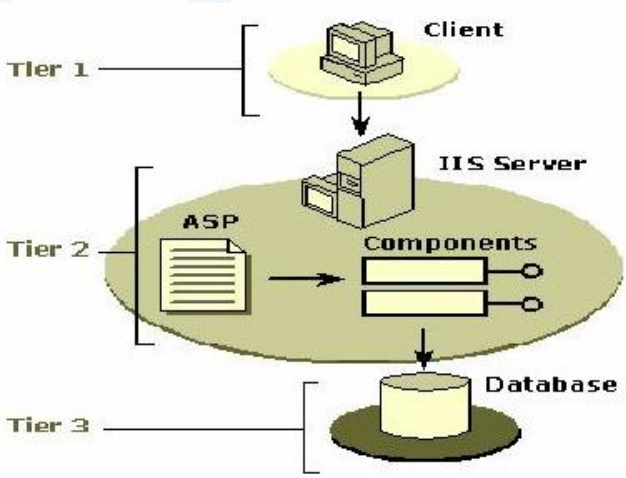
می آورد. Gateway موجود امکان استفاده از تمام قابلیت های نرم افزارهای وجود را فراهم نخواهد کرد و صرفا" پاسخگو به بخش محدودی از انتظارات خواهند بود. بدیهی است

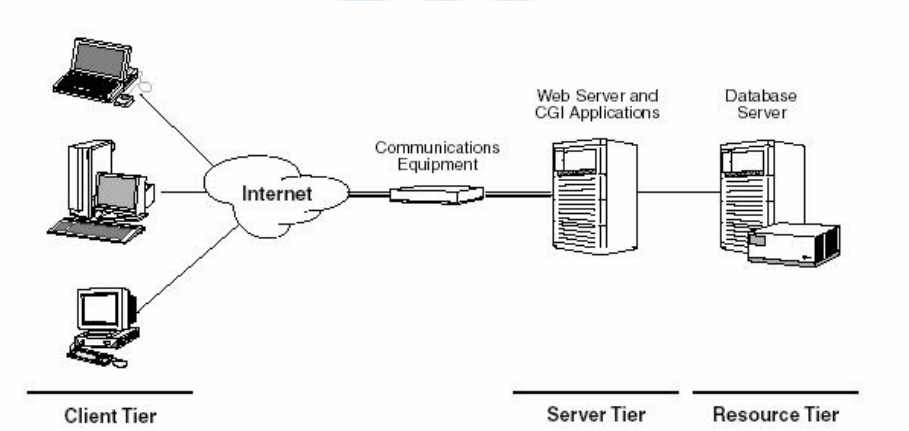
بخش هائی از نرم افزارهای موجود (سنتی) می بایست با رویکرد وب بازنویسی شده تا امکان ارتباط آنان با Gateway فراهم گردد.

برنامه های موجود بر روی برخی از سایت ها نظیر: خرید کالا، کتاب، رزو بلیط هواپیما ، ارسال و دریافت نامه الکترونیکی (نظیر hotmail) نمونه هائی از برنامه های مبتنی بر وب می باشند. در ادامه با برخی تعاریف برنامه های تحت وب آشنا می شویم:

- یک وب سایت که قادر به انجام عملیاتی خاص نظیر فروش کالا است.
- برنامه ای که بر روی وب اجراء می گردد.
- برنامه ای که بر روی یک سرویس دهنده وب در شبکه اجراء و امکان سرویس دهی به چندین کاربر در هر لحظه را دارا است.
- یک برنامه نرم افزاری که از پروتکل Http بعنوان هسته پروتکل ارتباطی خود بمنظور توزیع و ارائه اطلاعات مبتنی بر وب و با فرمت Html استفاده و آنان را برای کاربران ارسال خواهد کرد.
- یک برنامه مبتنی بر وب دارای لایه های زیر است:
  - یک لایه نازک سرویس دهنده (مرورگرهای وب)
  - یک لایه نمایش و ارائه (سرویس دهندگان وب)
  - یک لایه Application (سرویس دهنده Application)

- یک لایه بانک اطلاعاتی





ارائه یک مدل همگرا و جامع

برای پیاده سازی برنامه های تحت وب از تکنولوژی های متعدد و متفاوتی استفاده می گردد. بمنظور طراحی و پیاده سازی برنامه های مبتنی بر وب صرفا" یک روش وجود نداشته و می توان از روش های متعدد که هر یک برخاسته از تکنولوژی های متعددی می باشند ، به هدف خود دست پیدا کرد.

برخی از تکنولوژی های ارائه شده متعلق به شرکت های متعدد کامپیوتری بوده که در حالاتی ممکن است دارای عملکردهای مشابه باشند. کنسرسیوم وب مسئولیت استاندار

نمودن تکنولوژی های مرتبط در این زمینه را برعهده دارد. پس از استاندارد نمودن هر یک از تکنولوژی های موجود ، تمام تولیدکنندگان نرم افزار و سخت افزار سعی در رعایت موارد استاندارد شده کرده تا بدین طریق مخاطبان بیشتری را جذب و زمینه استفاده وسیع تر و گسترده از تکنولوژی های فوق ، فراهم گردد.
عملکرد اکثر برنامه های تحت وب در موارد بسیاری مشابه یکدیگر است:

ارائه یک بخش رابط کاربر بمنظور ارتباط با کاربران : دریافت خواسته ها و یا نمایش نتایج

دریافت و ارسال درخواست کاربران (از سرویس گیرنده بسمت سرویس دهنده)

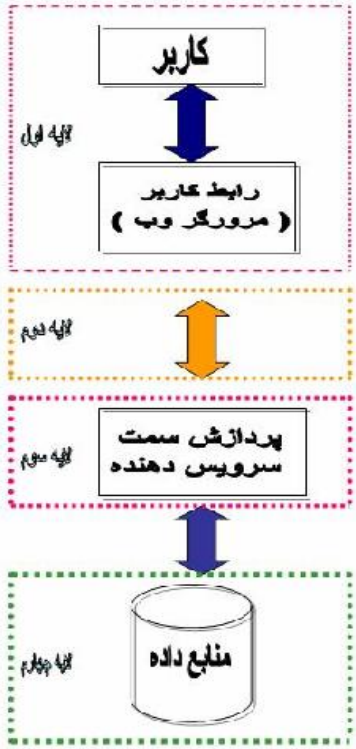
انجام پردازش لازم (مبتنی بر سرویس دهنده)

دستیابی به منابع داده ئی (بانک های اطلاعاتی) و انجام پردازش های لازم

ارسال نتایج بدستت آمده از پردازش های انجام شده برای سرویس گیرنده

انجام پردازش های لازم (مبتنی بر سرویس گیرنده)

شکل زیر نحوه انجام عملیات فوق را نشان می دهد:



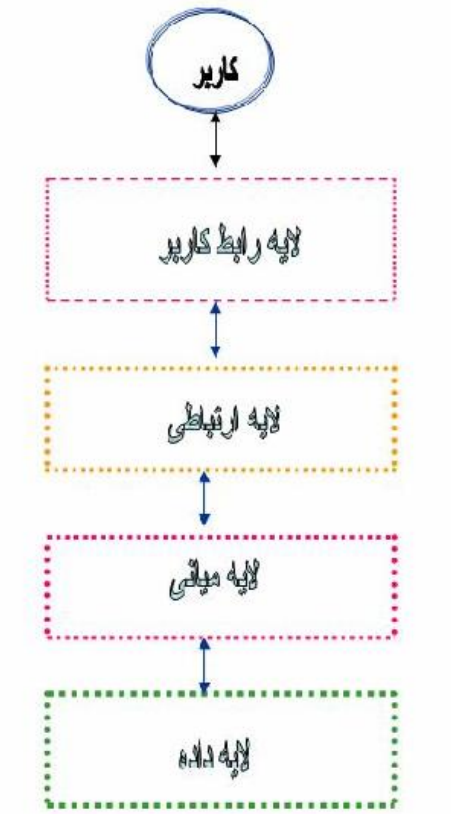
هدف ارائه یک مدل عملیاتی برای پیاده سازی برنامه های مبتنی بر وب می باشد. مدل پیشنهادی، مستقل از نوع تکنولوژی، ارائه شده است. در این مدل صرفنظر از نوع تکنولوژی استفاده شده، می توان تمامی عملیاتی را که یک برنامه مبتنی بر وب انجام می دهد را در چهار لایه متفاوت تبین و تعریف کرد.

لایه رابط کاربر

لایه ارتباطی

لایه میانی

لایه داده



هر یک از لایه های فوق مسئولیت انجام عملیات متفاوتی را برعهده داشته و در این راستا از تکنولوژی های متعددی استفاده می گردد. در ادامه، جایگاه هر یک از لایه های فوق در یک برنامه مبتنی بر وب تشریح و در ادامه به تبین جایگاه هر یک از تکنولوژی های موجود درلایه ها، پرداخته خواهد شد.

آشنائی با عملکرد هر لایه و شناخت تکنولوژی های موجود، زمینه شناخت اصولی، منطقی و سیستماتیک برنامه های مبتنی بر وب را بوجود خواهد آورد. دامنه استفاده از برخی تکنولوژی ها صرفا" در حد و اندازه یک لایه بوده و برخی دیگر از تکنولوژی ها دارای عماکردی فرا لایه ای بوده و ممکن است در چندین لایه استفاده گردند.

لایه رابط کاربر

لایه رابط کاربر بخشی از یک نرم افزار بوده که مسئولیت ارتباط با کاربران را برعهده دارد. کاربران با استفاده از امکانات لایه فوق ، قادر به برقراری ارتباط با نرم افزار و استفاده از امکانات و پتانسیل های موجود خواهند بود. لایه فوق دارای ویژگی های زیر است :

رابط کاربر بعنوان یک اینترفیس بین دنیای کاربران و دنیای کامپیوتر است.

بخش رابط کاربر برنامه های مبتنی بر وب با استفاده از برنامه های مرورگر، ارائه می گردد.

تمام بحث ها ی مربوط به لایه رابط کاربر ، با **مرورگرهای وب** آغاز می گردد.

اطلاعات ارسالی توسط سرویس دهنده وب توسط مرورگر وب نمایش داده می شود.

مرورگرهای وب دارای امکانات لازم برای تفسیر تگ های Html و نحوه نمایش آنان می باشند.

مرورگرهای وب با استفاده از فرم های وب امکان اخذ اطلاعات از کاربران و ارسال آنها برای سرویس دهنده را فراهم می آورند.

مرورگرهای وب پس از اخذ اطلاعات لازم از کاربران، با استفاده از متدهای GET و یا POST پروتکل HTTP، آنها را برای سرویس دهنده وب ارسال می نمایند.

مرورگرهای وب بمنظور پشتیبانی و نگهداری وضعیت یک برنامه از کوکی استفاده می نمایند.

تکنولوژی های موجود در این لایه وابسته به نوع مرورگر خواهند بود. ممکن است برخی از تکنولوژی ها توسط برخی از مرورگرها حمایت نشده و یا برخی از تکنولوژی ها از یک نسخه خاص در مرورگر پیش بینی شده باشند.

جایگاه مرورگرهای وب

مرورگرهای وب یکی از شاهکارهای اینترنت بوده که کاربران با استفاده از آنان قادر به استفاده از وب سایت ها و مشاهده صفحات وب می باشند. برنامه های فوق از جایگاه برنامه نویسی تحت وب دارای نقش بسیار مهمی می باشند. برنامه نویسان وب برای پیاده سازی بخش رابط کاربر برنامه های خود از امکانات گسترده این نوع نرم افزارها استفاده می نمایند.

تعاریف متفاوت مرورگرهای وب:

مرورگر وب، برنامه ای است که اطلاعات درخواست شده توسط کاربران اینترنت به اطلاع سرویس دهندگان وب رسانده و پس از اخذ اطلاعات، آنها را با یک فرمت تعریف شده بر روی صفحات نمایشگر کامپیوترهای کاربران، نمایش خواهند داد.

یک مرورگر وب، برنامه ای است که به متقاضی صفحات وب، امکان مشاهده صفحات و خواندن اطلاعات موجود را خواهد داد. برنامه های Internet Explorer (IE) و Navigator Netscape نمونه هائی متداول در این زمینه می باشند.

بمنظور مشاهده صفحات وب مربوط به یک وب سایت، از مرورگرهای وب استفاده می گردد. کاربران با استفاده از مرورگرهای وب، قادر به دریافت اطلاعات ارسالی توسط سرویس دهندگان وب و مشاهده آنان خواهند بود.

مرورگرهای وب، برنامه هائی می باشند که با استفاده از آنان امکان مشاهده صفحات وب، اخذ فایل و سایر عملیات مورد نیاز کاربران در زمان استفاده از اینترنت فراهم خواهد شد.

مرورگرها ، صفحات وب را که اغلب بصورت تگ های Html می باشند، خوانده و پس از تفسیر کدهای موجود، زمینه نمایش محتویات و اطلاعات موجود را فراهم می آورند.

مرورگرهای وب علاوه بر امکان تفسیر تگ های Html بمنظور تبین نحوه نمایش، دارای عناصر لازم بمنظور تفسیر اسکریپت های نوشته شده با یکی از زبانهای اسکریپت نیز می باشند.

جاوا اسکریپت و VBscript دو نمونه متداول از زبانهای اسکریپت بوده که در اکثر صفحات پویا دارای حضوری فعال می باشند.

نگرش کاربران معمولی و برنامه نویسان وب به مرورگرهای وب کاملا" متمایز بوده و هر یک با توجه نوع خواسته و انتظار خود از پتانسیل های موجود، استفاده خواهند کرد.

مرورگر InterNet Explorer

مرورگر Netscape Communicator

مرورگرها روند تکامل و شکل گیری

طراحی، پیاده سازی و توسعه مرورگرهای وب همزمان با مطرح شدن وب، آغاز و همچنان ادامه دارد

WorldWideWeb . این مرورگر توسط " تیم. برنرز لی " در سال ۱۹۹۰ و بر روی کامپیوتر NeXT در CERN نوشته گردید.

libwww . "تیم.برنرز لی " و دانشجوئی با نام " Jean-Francois Groff" از CERN در سال ۱۹۹۲، مرورگر WorldWideWeb را با استفاده از زبان برنامه نویسی C بازنویسی نمودند.

Line-Mode . دانشجوئی با نام "Nicola pellow" از دانشجویان ریاضی CERN در سال ۱۹۹۱ ، یک مرورگر خطی طراحی نمود که قابلیت استفاده بر روی دستگاههای متعدد را داشت. در ادامه "نیکلا" و دستیارانش امکان استفاده از مرورگر فوق را بر روی کامپیوترهای متنوعی (از یونیکس تا سیستم عامل DOS) فراهم نمودند.

ViolaWWW . در سال ۱۹۹۲ توسط دانشجوئی با نام "Pei Wei" از دانشگاه برکلی کالیفرنیا ، دومین مرورگر برای یونیکس طراحی گردید.

Midas . در سال ۱۹۹۲ توسط "Tony Johnson" در SLAC، سومین مرورگر برای سیستم های مبتنی بر یونیکس طراحی گردید. هدف از طراحی مرورگر فوق جمع آوری اطلاعات در رابطه با تحقیقات فیزیک بود.

Samba . اولین مرورگر برای کامپیوترهای مکینتاش که توسط " Robert Cailliau" طراحی و پیاده سازی گردید.نسخه نهائی و عملیاتی مرورگر فوق اواخر سال ۱۹۹۲ عرضه گردید.

موزائیک . مرورگر فوق توسط "Andreessen Marc" و "Eric Bina" از NCSA در سال ۱۹۹۳ برای سیستم های مبتنی بر X-Windows و بر روی کامپیوترهای یونیکس عرضه گردید. چند ماه بعد نسخه مرورگر فوق بمنظور اجراء بر روی سیستم های مکینتاش توسط "Aleks Totic" طراحی و عرضه گردید. موزائیک، اولین مرورگری با قابلیت استفاده بر روی پلات فورم های متعدد بود. این مرورگر دارای امکانات متعدد در رابطه با صوت، تصویر، فایل های سوابق و ... بود. مرورگر فوق پس از مدت زمان کوتاهی بعنوان رایج ترین مرورگر غیر اقتصادی مطرح گردید. در اگوست سال ۱۹۹٤ ، NCSA حق استفاده از مرورگر فوق را به شرکت Spyglass واگذار کرد. در ادامه شرکت فوق ، امتیاز استفاده از مرورگر موزائیک را به شرکت های دیگر نظیر ماکروسافت واگذار کرد. NCSA عملیات پیاده سازی و توسعه مرورگر موزائیک را در سال ۱۹۹۷ متوقف کرد.

Arena . در سال ۱۹۹۳، "Dave Raggett" در هیولت پاکارد (HP) شهر بریستول انگلستان، مرورگر فوق را طراحی و عرضه نمود. این مرورگر دارای قابلیت های فراوانی در رابطه با جداول و گرافیک بود.

Lynx . دانشگاه کانزاس یک مرورگر مستقل برای وب را طراحی نمود. هدف از طراحی مرورگر فوق توزیع اطلاعات در دانشگاه بود. در ادامه و در سال ۱۹۹۳، دانشجوئی با نام "Lou Montulli" یک اینترفیسی اینترنتی به برنامه فوق اضافه و نسخه شماره دو مرورگر وب Lynx را عرضه نمود. مرورگر فوق بسرعت متداول و بعنوان گزینه ای مناسب برای ترمینال های فاقد امکانات گرافیکی انتخاب و همچنان در این راستا از آن استفاده می گردد.

Opera . مرورگر فوق در سال ۱۹۹٤ توسط عده ای از محققین یک شرکت مخابراتی در اسلو نروژ، با نام Telenor طراحی گردید. در سال های بعد دو تن از اعضای گروه فوق ، از Telenor جدا شده و شرکت نرم افزاری Opera را با هدف تولید تجاری مرورگر فوق ، تاسیس کردند. نسخه Oper 2.1 در سال ۱۹۹٦ برای استفاده عموم کاربران اینترنت عرضه گردید.

InterNet In A Box . در سال ۱۹۹٤، O'Reilly و متحدانش، محصول فوق را عرضه نمودند. محصول فوق شامل تمامی نرم افزارهای ضروری و مورد نیاز کاربران برای استفاده از اینترنت بود. بدین ترتیب کاربران با نصب صرفا" یک برنامه از نصب و پیکربندی برنامه های متعدد برای دستیابی به اینترنت و امکانات موجود بی نیاز می شدند.

Mozilla . در اکتبر سال ۱۹۹٤ ، شرکت نت اسکیپ ، اولین نسخه مرورگر خود را با نام Mozilla 0.96b عرضه نمودند. (نسخه فوق نسخه بتا بود). در دسامبر همان سال ،نسخه نهائی مرورگر فوق با نام Mozilla ۱،۰ عرضع گردید. مرورگر فوق اولین مرورگر تجاری در عرصه اینترنت است .

Internet Explorer . در اگوست سال ۱۹۹۵، شرکت ماکروسافت همزمان با معرفی ویندوز ۹۵ ، مرورگر فوق را عرضه نمود. مرورگر فوق بهمراه مرورگر شرکت نت اسکیپ متداولترین نوع مرورگرهای وب بوده که توسط اکثر کاربران اینترنت در حال حاضر استفاده می گردند.

- برنامه های مبتنی بر وب شامل درخواست هائی از طرف مرورگرهای وب برای سرویس دهندگان وب می باشند. مرورگرها برای ارسال درخواست خود از پروتکل

Http و یا سایر پروتکل های استاندارد استفاده می نمایند. استفاده از واژه "مرورگر " برای این نوع نرم افزارها چندان منطقی بنظر نمی رسد ، چراکه برنامه های فوق علاوه بر امکان بازیابی و نمایش اطلاعات ، دارای قابلیت های متعدد و فراوانی در رابطه با برنامه نویسی مبتنی بر وب می باشند.

برنامه های فوق بمنزله یک اینترفیس مناسب برای پردازش و انجام عملیات متفاوت ایفای وظیفه می نمایند. برنامه نویسان وب بدون شناخت و توجه به پتانسیل و امکانات مرورگرها، قادر به آفرینش آثار ماندگار، خود نخواهند بود.

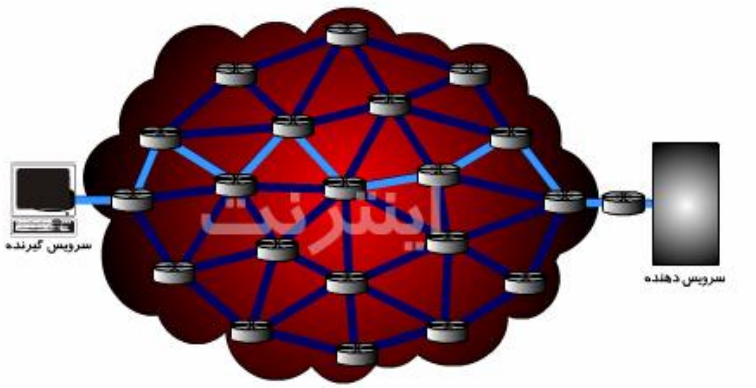
مقایسه امکانات مرورگرهای متفاوت با توجه به نوع سیستم عامل

XML	Table color	I frames	dhtml	gif89	CSS	java script	font color	font size	plug-ins	tables	frames	java	browsers
Windows													
n	n	n	n	n	n	N	y	y	n	y	y	n	AOL 3.0
n	n	n	n	n	n	N	n	n	n	n	n	n	AOL 1.0
y	y	y	y	y	y	Y	y	y	y	y	y	y	IE 5.5
s	y	y	y	y	y	Y	y	y	y	y	y	y	IE 5.0
n	y	y	y	y	y	Y	y	y	y	y	y	y	IE 4.0
n	y	y	n	y	y	Y	y	y	y	y	y	y	IE 3.0
n	n	n	n	n	n	N	y	y	n	y	n	n	IE 2.0
n	n	n	n	n	n	N	y	y	n	y	n	n	IE 1.0
n	n	n	n	n	n	N	n	y	n	y	y	n	Mosaic 3.0
n	n	n	n	n	n	N	n	n	n	n	n	n	Mosaic 1.0
y	y	n	y	y	y	Y	y	y	y	y	y	y	NS 6
n	y	n	y	y	y	Y	y	y	y	y	y	y	NS 4.7
n	y	n	y	y	y	Y	y	y	y	y	y	y	NS 4.5
n	y	n	n	y	n	Y	y	y	y	y	y	y	NS 3.0
n	n	n	n	y	n	S	y	y	y	y	y	y	NS 2.0
n	n	n	n	n	n	N	n	y	n	y	n	n	NS 1.1
y	y	n	n	y	y	Y	y	y	s	y	y	y	Opera 4.2
n	y	n	n	y	y	Y	y	y	y	y	y	n	Opera 3.60
n	y	n	n	y	n	Y	y	y	y	y	y	n	Opera 3.5
n	n	n	n	n	n	N	n	n	n	y	y	n	Lynx
Macintosh													
XML	Table color	I frames	dhtml	gif89	CSS	java script	font color	font size	plug-ins	tables	frames	java	browsers
n	n	n	n	n	n	N	n	n	n	n	n	n	AOL 2.7
n	n	n	n	n	n	N	n	n	n	n	n	n	AOL 1.0
n	n	n	n	y	n	N	y	y	n	y	y	n	Cyberdog 2.0
s	y	y	y	y	y	Y	y	y	y	y	y	y	IE 5.0
n	y	y	y	y	y	Y	y	y	y	y	y	y	IE 4.0
n	y	y	n	y	y	Y	y	y	y	y	y	y	IE 3.0
n	n	n	n	n	n	N	y	y	y	y	y	n	IE 2.0
n	n	n	n	n	n	N	y	y	n	y	y	n	Mosaic 3.07
n	n	n	n	n	n	N	n	n	n	y	n	n	Mosaic 2.0
n	n	n	n	n	n	N	n	n	n	n	n	n	Mosaic 1.0
y	y	n	y	y	y	Y	y	y	y	y	y	y	NS 6
n	y	n	y	y	y	Y	y	y	y	y	y	y	NS 4.74
n	y	n	y	y	y	Y	y	y	y	y	y	y	NS 4.5

n	y	n	y	y	s	Y	y	y	y	y	y	y	NS 4.06
n	y	n	n	y	s	Y	y	y	y	y	y	y	NS 3.0
n	n	n	n	y	n	S	y	y	y	y	y	n	NS 2.0
n	n	n	n	n	n	N	n	y	n	y	n	n	NS 1.1
Unix													
XML	Table color	I frames	dhtml	gif89	CSS	java script	font color	font size	plug-ins	tables	frames	java	browsers
y	y	y	y	y	y	Y	y	y	y	y	y	y	IE 4.01
n	y	y	y	y	y	Y	y	y	y	y	y	y	IE 4.01
n	n	n	n	n	n	N	n	n	n	y	n	n	Mosaic 2.75
n	n	n	n	n	n	N	n	n	n	n	n	n	Mosaic 1.0
y	y	n	y	y	n	Y	y	y	y	y	y	y	NS 4.6
n	y	n	y	y	n	Y	y	y	y	y	y	y	NS 4.06
n	n	n	n	y	n	Y	y	y	y	y	y	y	NS 3.0
n	n	n	n	y	n	S	y	y	y	y	y	y	NS 2.0
n	n	n	n	n	n	N	n	y	n	y	n	n	NS 1.1
n	n	n	n	n	y	N	n	y	n	y	n	n	Arena 3
n	n	n	n	n	n	N	n	n	n	y	y	n	Lynx
Linux													
XML	Table color	I frames	dhtml	gif89	CSS	java script	font color	font size	plug-ins	tables	frames	java	browsers
y	y	n	y	y	y	Y	y	y	y	y	y	y	NS 6
y	y	n	n	y	y	Y	y	y	y	y	y	s	Mozilla
n	n	y	n	s	y	Y	y	y	y	y	y	y	NS 4.7
y	y	n	n	y	y	N	y	y	n	y	y	n	Amaya
y	y	n	n	y	y	N	y	y	s	y	y	n	Opera 4a
n	n	n	n	n	n	N	n	n	n	y	y	n	Lynx
Television													
XML	Table color	I frames	dhtml	gif89	CSS	java script	font color	font size	plug-ins	tables	frames	java	browsers
n	y	n	n	y	n	Y	y	y	n	y	y	n	WebTV
NextStep													
XML	Table color	I frames	dhtml	gif89	CSS	java script	font color	font size	plug-ins	tables	frames	java	browsers
n	n	n	s	n	n	n	y	y	n	y	y	n	OmniWeb 2.1
n	n	n	n	n	n	n	y	y	n	n	n	n	OmniWeb 1.0
OS/2													
XML	Table color	I frames	dhtml	gif89	CSS	java script	font color	font size	plug-ins	tables	frames	java	browsers
n	n	n	n	y	n	n	y	y	n	y	n	n	NS 2.02
n	n	n	n	n	n	n	y	y	n	y	n	n	Web IE 1.1
n	n	n	n	y	n	y	y	y	n	y	y	n	Opera
n	n	n	n	n	n	n	n	n	n	y	y	n	Lynx

زیر ساخت اینترنت

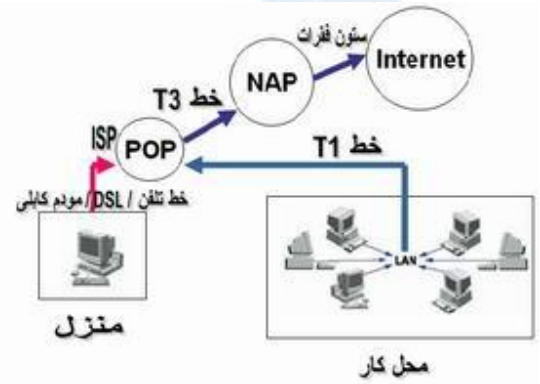
اینترنت از مجموعه ای شبکه کامپیوتری (بزرگ ، کوچک) تشکیل شده است. شبکه های فوق با روش های متفاوتی به یکدیگر متصل و موجودیت واحدی با نام "اینترنت" را بوجود آورده اند. نام در نظر گرفته شده برای شبکه فوق از ترکیب واژه های "**Inter**connected" و"**Net**work" انتخاب شده است. (شبکه های بهم مرتبط). اینترنت فعالیت اولیه خود را از سال ۱۹۶۹ و با چهار دستگاه کامپیوتر میزبان (host) آغاز و پس از رشد باورنکردنی خود، تعداد کامپیوترهای میزبان در شبکه به بیش از ده ها میلیون دستگاه رسیده است. اینترنت به هیچ سازمان و یا موسسه خاصی در جهان تعلق ندارد. عدم تعلق اینترنت به یک سازمان ویا موسسه به منزله عدم وجود سازمانها و انجمن های خاصی برای استانداردسازی نیست .یکی از این انجمن ها، "انجمن اینترنت" است که در سال ۱۹۹۲ با هدف تبین سیاست ها و پروتکل های مورد نظر جهت اتصال به شبکه تاسیس شده است.



روترها، مسئولیت تعیین مسیر بین سرویس گیرندگان و سرویس دهندگان در اینترنت را بر عهده دارند.

سلسله مراتب شبکه های کامپیوتری

هر کامپیوتری که به شبکه اینترنت متصل می گردد، بخشی از شبکه تلـــــقی می گردد. مثلا" می توان با استفاده از تلفن (منزل) به یک مرکز ارائه دهنده خدمات اینترنت (ISP) متصل و از اینترنت استفاده کرد. در چنین حالتی کامپیوتر مورد نظر بعنوان بخشی از شبکه بزرگ اینترنت محسوب خواهد شد. .برخی از کاربران در ادارات خود و با استفاده از بستر ایجاد شده، به اینترنت متصل می گردند. در مدل فوق، کاربران در ابتدا از شبکه محلی نصب شده در سازمان استفاده می نمایند. شبکه فوق با استفاده از خطوط مخابراتی خاص و یا سایر امکانات مربوطه به یک مرکز ارائه دهنده خدمات اینترنت متصل شده است. مرکز ارائه دهنده خدمات اینترنت نیز ممکن است به یک شبکه بزرگتر متصل شده باشد. اینترنت، شبکه ای است که از شبکه های بیشماری تشکیل شده است (شبکه ای از سایر شبکه ها)



اکثر شرکت های مخابراتی بزرگ دارای ستون فقرات اختصاصی برای ارتباط ناحیه های متفاوت می باشند. در هر ناحیه ، شرکت مخابراتی دارای یک " نقطه حضور" (**POP**: Point of Presence) است. POP ، مکانی است که کاربران محلی با استفاده از آن به شبکه شرکت مخابراتی متصل می گردند. (به منظور ارتباط با شبکه از خطوط تلفن معمولی و یا خطوط اختصاصی استفاده می گردد).

در مدل فوق، چندین شبکه سطح بالا وجود داشته که توسط " نقاط دستیابی شبکه" (**NAP**: Network Access Points) به یکدیگر مرتبط می گردند.

فرض کنید، شرکت A یک مرکزارائه دهنده خدمات اینترنت بزرگ باشد. درهر شهرستان اصلی، شرکت A دارای یک POP است. هر یک از POP ها دارای امکانات گسترده ای به منظور تماس کاربران محلی می باشند. شرکت A به منظور اتصال POP ها بیکدیگر و شرکت، از خطوط اختصاصی فیبر نوری استفاده می نماید. فرض کنید شرکت B، یک مرکز ارائه دهنده خدمات اینترنت همکارباشد.شرکت B ، ساختمانهای بزرگی را در شهرهای اصلی ایجاد و ماشین های سرویس دهنده اینترنت را در آنها مستقر نموده است. شرکت B از خطوط اختصاصی فیبـــرنوری برای ارتباط ساختـمانهای استفـــاده می نماید. در مدل فوق، تمام مشترکین شرکت A قادر به برقراری ارتباط با یکدیگر خواهند بود. وضعیت مشترکین شرکت B نیز مشابه مشترکین شرکت A است. آنها نیز قادر به برقراری ارتباط با یکدیگر خواهند بود. در چنین حالتی امکان برقراری ارتباط بین مشترکین شرکت A و مشترکین شرکت B وجود ندارد. بدین منظور شرکت های A و B تصمیم می گیرند از طریق NAP در شهرهای متفاوت بیکدیگر متصل گردند. ترافیک موجود بین دو شرکت از طریق شبکه های داخلی و NAP انجام خواهد شد.

در اینترنت، هزاران مرکز ارائه دهنده سرویس اینترنت بزرگ از طریق NAP در شهرهای متفاوت بیکدیگر متصل می گردند. در نقاط فوق (NAP) روزانه میلیاردها بایت اطلاعات جابجا می گردد. اینترنت ، مجموعه ای از شبکه های بسیار بزرگ بوده که تمام آنها از طریق NAP بیـــکدیگر مرتبط می گردند. در چنین حالتی هر کامپیوتر موجود در اینترنت قادر به ارتباط با سایر کامپیوترهای موجود در شبکه خواهد بود.

تمام شبکه های کامپیوتری از طریق NAP، ستون فقرات ایجاد شده و روتر قادر به ارتباط بایکدیگر خواهند بود. پیام ارسالی توسط یک کاربر اینترنت از چندین شبکه متفاوت عبور تا به کامـــپیوتر مورد نظر برســد. فرآیند فوق در کمتر از یک ثانیه انجام خواهد شد.

روتر، مسیریک بسته اطلاعاتی ارسالی توسط یک کامپیوتر برای کامپیوتر دیگر را تعیین می کند. روترها کامپیوترهای خاصی می باشند که پیام های ارسال شده توسط کاربران اینترنت با وجود هزاران مسیر موجود را مسیریابی و در اختیار دریافت کنندگان مربوطه قرار خواهد داد. روتر دو کار اساسی را در شبکه انجام می دهد:

- ایجاد اطمینان در رابطه با عدم ارسال اطلاعات به مکانهائی که به آنها نیاز نمی باشد.
- اطمینان از ارسال صحیح اطلاعات به مقصد مورد نظر

روترها به منظور انجام عملیات فوق، می بایست دو شبکه مجزا را بیکدیگر متصل نمایند. روتر باعث ارسال اطلاعات یک شبکه به شبکه دیگر ، حفاظت شبکه ها از یکدیگر و پیشگیری از ترافیک می گردد. با توجه به اینکه اینترنت از هزاران شبکه کوچکتر تشکیل شده است، استفاده از روتر یک ضرورت است.

در سال ۱۹۸۷ موسسه NSF ، اولین شبکه با ستون فقرات پر سرعت را ایجاد کرد. شبکه فوق NSFNET نامیده شد. در این شبکه از یک خط اختصاصی T1 استفاده و ۱۷۰ شبکه کوچکتر بیکدیگر متصل می گردیدند. سرعت شبکه فوق ۱،٥٤٤ مگابیت در ثانیه بود. در ادامه شرکت های IBM ، MCI و Merit ، شبکه فوق را توسعه و ستون فقرات آن را به T3 تبدیل کردند(٤٥ مگابیت در ثانیه). برای ستون فقرات شبکه از خطوط فیبرنوری (fiber optic trunk) استفاده گردید.هر trunk از چندین کابل فیبر نوری تشکیل می گردد(به منظور افزایش ظرفیت).

پروتکل اینترنت

هر ماشین موجود در اینترنت دارای یک شماره شناسائی منحصر بفرد است. این شماره شناسائی ، آدرس IP(Internet Protocol) نامیده می گردد. پروتکل فوق مشابه یک زبان ارتباطی مشترک برای گفتگوی کامپیوترهای موجود در اینترنت است . پروتکل

، به مجموعه قوانینی اطلاق می گردد که با استناد به آن گفتگو و تبادل اطلاعاتی بین دو کامپیوتر میسر خواهد شد. IP دارای فرمتی بصورت :۲۱۱،۲۷،٦٥،۱۳۸ است.

بخاطر سپردن آدرس های IP به منظور دستیابی به کامپیوتر مورد نظر، مشکل است.

بدین منظور هر کامپیوتر دارای نام انحصاری خود شده و از طریق سیستمی دیگر، آدرس IP به نام درنظر گرفته شده برای کامپیوتر، نسبت داده می شود.

در آغاز شکل گیری اینترنت، تعداد کامپیوترهای موجود در شبکه بسیار کم بود و هر کاربر که قصد استفاده از شبکه را داشت، پس از اتصال به شبکه از آدرس IP کامپیوتر مورد نظر برای برقراری ارتباط استفاده می کرد. روش فوق مادامیکه تعداد کامپیوترهای میزبان کم بودند، مفید واقع گردید ولی همزمان با افزایش تعداد کامپیوترهای میزبان در شبکه اینترنت، کارآئی روش فوق بشدت افت و غیرقابل استفاده گردید. به منظور حل مشکل فوق از یک فایل ساده متنی که توسط " مرکز اطلاعات شبکه " (NIC) پشتیبانی می گردید، استفاده گردید. بموازات رشد اینترنت و ورود کامپیوترهای میزبان بیشتر در شبکه ، حجم فایل فوق افزایش و بدلیل سایر مسائل جانبی ، عملا" استفاده از روش فوق برای برطرف مشکل " **تبدیل نام به آدرس** " فاقد کارآئی لازم بود. درسال ۱۹۸۳ ، سیستم DNS(Domain Name System) ارائه گردید. سیستم فوق مسئول تطبیق نام به آدرس، بصورت اتوماتیک است . بدین ترتیب کاربران اینترنت به منظور اتصال به یک کامپیوتر میزبان ، صرفا" می توانند نام آن را مشخص کرده و با استفاده از DNS، آدرس IP مربوطه آن مشخص تا زمینه برقراری ارتباط فراهم گردد.

منظور از " نام" چیست ؟

در زمان استفاده از وب و یا ارسال یک E-Mail از یک "نام حوزه" استفاده می گـــردد. مـــــثلا" URL(Uniform Resource Locator) مربـــــــــــــــــوط به http://www.oursite.com شامل " نام حوزه " oursite.com است.

درزمان استفاده از "نام حوزه "، می بایست از سرویس دهندگان DNS به منظور ترجـمه

نام به آدرس استفاده شود. سرویس دهندگان DNS درخواست هائی را از برنامه ها و یا سایر سرویس دهندگان DNS به منظور تبدیل نام به آدرس دریافت می نمایند. سرویس دهنده DNS در زمان دریافت یک درخواست، بر اساس یکی از روش های زیر با آن برخورد خواهد کرد:

- قادر به پاسخ دادن به درخواست است. IP مورد نظر برای نام درخواست شده را می داند .
- قادر به ارتباط با یک سرویس دهنده DNS دیگر به منظور یافتن آدرس IP نام درخواست شده است.(عملیات فوق ممکن است تکرارگردد)
- اعلام " عدم آگاهی از آدرس IP درخواست شده " و مشخص کردن آدرس IP یک سرویس دهنده DNS دیگر که آگاهی بیشتری دارد.
- ارائه یک پیام خطاء در رابطه با عدم یافتن آدرس برای نام درخواست شده

فرض نمائید، آدرس http://www.oursite.com در برنامه مرورگر (IE) تایپ شده باشد. مرورگر با یک سرویس دهنده DNS به منظور دریافت آدرس IP ارتباط برقرار می نماید. سرویس دهنده DNS عملیات جستجو برای یافتن آدرس IP را از یکی از سرویس دهندگان DNS سطح ریشه ، آغاز می نماید. سرویس دهندگان ریشه، از آدرس های IP تمام سرویس دهندگان DNS که شامل بالاترین سطح نامگذاری حوزه ها (COM، NET، ORG و ...) آگاهی دارند. سرویس دهنده DNS، درخواست آدرس http://www.oursite.com را نموده و سرویس دهنده ریشه اعلام می نماید که " من آدرس فوق را نمی دانم ولی آدرس IP مربوط به سرویس دهنده COM این است ". در ادامه سرویس دهنده DNS شما با سرویس دهنده DNS مربوط به حوزه COM ارتباط و درخواست آدرس IP سایت مورد نظر را می نماید .سرویس دهنده فوق آدرس های IP مربوط به سرویس دهنده ای که قادر به در اختیار گذاشتن آدرس IP سایت مورد نظر است را در اختیار سرویس دهنده DNS شما قرار خواهد داد. در ادامه سرویس دهنده DNS با سرویس دهنده DNS مربوطه تماس و

درخواست آدرس IP سایت مورد نظر را می نماید، سرویس دهنده DNS آدرس IP سایت درخواست شده را در اختیار سرویس دهنده DNS شما قرار خواهد داد. با مشخص شده آدرس IP سایت مورد نظر ، امکان اتصال به سایت فراهم خواهد شد. از نکات قابل توجه سیستم فوق، وجود چندین سرویس دهنده هم سطح DNS است .بنابراین در صورتیکه یکی از آنها با اشکال مواجه گردد، از سایر سرویس دهندگان به منظور ترجمه نام به آدرس استفاده می گردد. یکی دیگر از ویژگی های سیستم فوق، امکان Cacheing است. زمانیکه یک سرویس دهنده DNS به یک درخواست پاسخ لازم را داد، آدرس IP مربوطه ای را Cache خواهد کرد. در ادامه زمانیکه درخواستی برای یکی از حوزه های COM واصل گردد، سرویس دهنده DNS از آدرس Cache شده استفاده خواهد کرد.

سرویس دهندگان DNS روزانه به میلیاردها درخواست پاسخ می دهند. سیستم فوق از یک بانک اطلاعاتی توزیع شده به منظور ارائه خدمات به متقاضیان استفاده می نماید.

سرویس دهندگان وب

امکانات و سرویس های موجود بر روی اینترنت از طریق سرویس دهندگان اینترنت انجام می گیرد. تمام ماشین های موجود در اینترنت سرویس دهنده و یا سرویس گیرنده می باشند. ماشین هائی که برای سایر ماشین ها، خدماتی را ارائه می نمایند، سرویس دهنده نامیده می شوند. ماشین هائی که از خدمات فوق استفاده می نمایند، سرویس گیرنده می باشند. اینترنت شامل سرویس دهندگان متعددی نظیر سرویس دهنده وب، سرویس دهنده پست الکترونیکی و ... به منظور پاسخگوئی به نیازهای متعدد کاربران اینترنت می باشد.

زمانیکه به یک وب سایت متصل و درخواست یک صفحه اطلاعات می شود، کامپیوتر درخواست کننده بمنزله یک سرویس گیرنده تلقی می گردد. در این حالت درخواست شما (بعنوان سرویس گیرنده) در اختیار سرویس دهنده وب گذاشته می شود. سرویس

دهنده صفحه درخواستی را پیدا و آن را برای متقاضی ارسال خواهد داشت. در مدل فوق کاربران و سرویس گیرندگان از یک مرورگر وب برای اعلام درخواست خود استفاده و سرویس دهندگان وب مسئول دریافت درخواست و ارسال اطلاعات مورد نظر برای سرویس گیرندگان می باشند.

یک سرویس دهنده دارای یک آدرس IP ایستا (ثابت) بوده که تغییر نخواهد کرد. کامپیوتری که با استفاده از آن به اینترنت متصل می گردید ، دارای یک IP متغیر بوده که توسط ISP مربوطه به شما اختصاص داده می شود. آدرسIP تخصیص یافته در طول مدت اتصال به اینترنت (یک جلسه کاری) ثابت بوده و تغییر نخواهد کرد. آدرس IP نسبت داده به شما در آینده و تماس مجدد با ISP ممکن است تغییر نماید. مراکز ISP برای هر یک از پورت های خود یک IP ایستا را نسبت می دهند. بدیهی است در آینده با توجه به پورت مورد نظر که در اختیار شما قرار داده می شود، ممکن است آدرس IP نسبت به قبل متفاوت باشد.

هر یک از سرویس دهندگان، سرویس های خود را از طریق پورت های مشخصی انجام می دهند. مثلا" در صورتیکه بر روی یک ماشین، سرویس دهندگان وب و FTP مستقر شده باشند، سرویس دهنده وب معمولا" از پورت ۸۰ و سرویس دهنده FTP از پورت ۲۱ استفاده می نمایند. در چنین حالتی سرویس گیرندگان از خدمات یک سرویس خاص که دارای یک آدرس IP و یک شماره پورت منحصر بفرد است، استفاده می نمایند. زمانیکه سرویس گیرنده، از طریق یک پورت خاص به یک سرویس متصل می گردد، به منظور استفاده از سرویس مورد نظر، از یک پروتکل خاص استفاده خواهد شد.. پروتکل ها اغلب بصورت متنی بوده و نحوه مکالمه بین سرویس گیرنده و سرویس دهنده را تبین می نمایند. سرویس گیرنده وب و سرویس دهنده وب از پروتکل **HTTP**(Hypertext Transfer Protocol) برای برقراری مکالمه اطلاعاتی بین خود، استفاده می نمایند.

شبکه ها، روترها، NAPs، ISPs، سرویس دهندگان DNS و سرویس دهندگان قدرتمند، همگی سهمی در شکل گیری و سرویس دهی بزرگترین شبکه موجود در سطح جهان (اینترنت) را برعهده دارند. عناصر فوق در زندگی مدرن امروزی جایگاهی ویژه دارند. بدون وجود آنها، اینترنتی وجود نخواهد داشت و بدون وجود اینترنت، زندگی امروز بشریت را تعریفی دیگر لازم است!

ISP

مراکز ارائه دهنده خدمات اینترنت (**ISP**)، خدمات متعددی نظیر پست الکترونیکی و دستیابی به اینترنت را در اختیار متقاضیان قرار می دهند. در زمان انتخاب یک ISP می بایست فاکتورهای متعددی را بررسی نمود. امنیت، نوع و کیفیت سرویس های ارائه شده و قیمت ارائه خدمات از جمله فاکتورهای مهم در زمان انتخاب یک ISP است.

ISP چیست ؟

یک ISP و یا Internet Service Provider ، شرکتی است که امکان دستیابی به اینترنت و سایر سرویس های وب را فراهم می نماید. مراکز ارائه دهنده خدمات اینترنت علاوه بر نگهداری و پشتیبانی از یک خط مستقیم به اینترنت، فعالیت های متعدد دیگری نظیر نگهداری و پشتیانی از سرویس دهندگان وب را نیز انجام می دهند. مراکز فوق با ارائه نرم افزارهای لازم (در صورت ضرورت)، یک رمز عبور حفاظت شده و یک شماره تلفن برای تماس با شبکه، امکان استفاده از اینترنت و مبادله نامه های الکترونیکی را در اختیار متقاضیان قرار می دهند. برخی از مراکز ISP خدمات اضافه دیگری را نیز ارائه می نمایند.

مراکز ISP دارای ابعاد و اندازه های متفاوتی می باشند. برخی از آنان توسط افرادی اندک اداره می شوند و تعدادی دیگر شرکت هائی بزرگ می باشند که خدمات متنوعی را در اختیار کاربران قرار می دهند . مراکز ارائه دهند خدمات اینترنت دارای حوزه های عملیاتی متفاوتی نیز می باشند. مثلا" برخی از آنان خدمات خود را صرفا" در سطح یک شهرستان ارائه داده و برخی دیگر دارای قابلیت های منطقه ای و حتی بین المللی می باشند.

مراکز ISP چه سرویس هائی را ارائه می دهند ؟

همانگونه که اشاره گردید، خدماتی که توسط مراکز ارائه دهنده خدمات اینترنت ارائه میگردد بسیار متنوع و در عین حال متفاوت است:

- تقریبا" تمامی مراکز ارائه دهنده خدمات اینترنت، سرویس هائی نظیر پست الکترونیکی و استفاده از اینترنت را ارائه می نمایند.
- نوع و کیفیت ارائه خدمات و پشتیبانی فنی توسط مراکز ارائه دهنده خدمات اینترنت دارای سطوح متفاوتی است.
- اکثر مراکز ISP ، سرویس هاستینگ وب را نیز ارائه می نمایند. با استفاده از سرویس فوق ، متقاضیان می توانند صفحات وب شخصی خود را ایجاد و از آنان نگهداری نمایند . اختصاص فضای لازم به منظور ذخیره سازی اطلاعات از جمله وظایف یک ISP در این رابطه است.
- برخی از مراکز ارائه دهنده خدمات اینترنت سرویس هائی را به منظور طراحی و پیاده سازی صفحات وب ارائه می نمایند.
- تعدادی از مراکز ISP گزینه های متفاوتی را در ارتباط با نوع دستیابی به اینترنت در اختیار متقاضیان قرار می دهند. (Dial-up ، DSL ، مودم های کابلی). برخی از مراکز ISP امکان دستیابی به اینترنت را صرفا" از طریق خطوط معمولی تلفن فراهم می نمایند.
- اکثر مراکز ISP عملیات متفاوتی نظیر تهیه Backup از نامه های الکترونیکی و فایل های وب را نیز انجام می دهند . در صورتی که بازیافت نامه های الکترونیکی و فایل های وب برای شما مهم است (در صورت بروز اشکال)، یک ISP را انتخاب نمائید که Backup گرفتن از داده ها را در دستور کار خود قرار داده است.

چگونه یک ISP را انتخاب نمائیم؟

برای انتخاب یک ISP پارامترهای متعددی بررسی می گردد:

- **امنیت** : آیا ISP انتخابی از رویکردهای مناسب امنیتی در جهت حفاظت اطلاعات استفاده می نماید ؟ آیا از رمزنگاری و SSL به منظور حفاظت اطلاعات ارسالی شما نظیر نام و رمز عبور استفاده می گردد؟
- **محرمانگی** : آیا ISP انتخابی دارای یک سیاست تعریف شده در خصوص رعایت حریم خصوصی کاربران است ؟ آیا خیال شما از این بابت راحت است که چه افرادی به اطلاعات شما دستیابی دارند؟ نحوه برخورد و استفاده آنان از اطلاعات به چه صورت است؟
- **سرویس ها** : آیا ISP انتخابی سرویس های مورد نظر شما را ارائه می نماید؟ آیا سرویس های ارائه شده تامین کننده نیاز شما می باشند؟ آیا پشتیبانی لازم به منظور ارائه سرویس ها در اختیار شما گذاشته می شود؟
- **قیمت** : آیا قیمت ارائه خدمات توسط ISP قابل قبول است؟ آیا قیمت ارائه شده با توجه به تعداد و نوع سرویس های ارائه شده، منطقی است؟ آیا به منظور دریافت خدمات ارزان تر، از کیفیت و امنیت چشم پوشی می نمائید؟
- **اعتماد پذیری** : آیا به سرویس های ارائه شده توسط ISP انتخابی می توان اعتماد داشت و یا در اغلب موارد سرویس های مورد نظر به دلایل متفاوتی نظیر پشتیبانی و نگهداری، تعداد زیاد کاربران و ...، غیر فعال بوده و عملا" امکان استفاده از آنان وجود ندارد. در صورتی که به دلایل متفاوتی لازم است برخی از سرویس های ارائه شده غیر فعال گردند آیا این موضوع با استفاده از مکانیزم های خاصی به شما اطلاع داده می شود؟
- **پشتیبانی کاربران** : آیا ISP انتخابی دارای بخش پشتیبانی کاربران است؟ نحوه برخورد پرسنل بخش پشتیبانی به چه صورت است؟ آیا آنان دارای دانش لازم به منظور پاسخگوئی منطقی به سوالات شما می باشند؟

- **سرعت** : سرعت اتصال ISP انتخابی به اینترنت چگونه است ؟ آیا این سرعت به منظور دستیابی شما به نامه های الکترونیکی و استفاده از وب کافی است؟
- **کیفیت ارائه خدمات** : آیا ISP انتخابی دارای عملکردی مثبت در کارنامه فعالیت خود است و استفاده کنندگانی که قبلاً از خدمات آنان استفاده نموده اند، از کیفیت ارائه خدمات راضی می باشند؟

DSL

برای اتصال به اینترنت از روش های متفاوتی استفاده می گردد. استفاده از مودم معمولی، مودم کابلی، شبکه محلی و یا خطوط DSL(Digital Subscriber Line)، نمونه هائی از روش های موجود برای اتصال به اینترنت می باشند. DSL ، یک اتصال با سرعت بالا را با استفاده از کابل های معمولی تلفن برای کاربران اینترنت فراهم می نماید.

مزایای DSL

- در زمان اتصال به اینترنت، امکان استفاده از خط تلفن برای تماس های مورد نظر همچنان وجود خواهد داشت.
- دارای سرعتی بمراتب بالاتر از مودم های معمولی است (۵/۱ مگابایت).
- نیاز به کابل کشی جدید نبوده و همچنان می توان از خطوط تلفن موجود استفاده کرد.
- شرکت ارائه دهنده DSL ، مودم مورد نظر را در زمان نصب خط فوق در اختیار مشترک قرار خواهد داد.

اشکالات DSL

- یک اتصال DSL هر اندازه که به شرکت ارائه دهنده سرویس فوق نزدیکتر باشد، دارای کیفیت بهتری است.
- سرعت دریافت داده نسبت به ارسال داده بمراتب بیشتر است (عدم وجود توا زن منطقی)
- سرویس فوق در هر محل قابل دسترس نمی باشد.

مبانی DSL

در زمان نصب یک تلفن (استاندارد) در اغلب کشورها از یک زوج کابل مسی استفاده می شود. کابل مسی دارای پهنای بمراتب بیشتری نسبت به آن چیزی است که در مکالمات تلفنی استفاده می گردد (بخش عمده ای ازظرفیت پهنای باند استفاده نمی گردد). DSL از پهنای باند بلااستفاده بدون تاثیر گذاری منفی بر کیفیت مکالمات صوتی، استفاده می نماید. (تطبیق فرکانس های خاص به منظورانجام عملیات خاص). به منظور شناخت نحوه عملکرد DSL ، لازم است در ابتدا با یک خط تلفن معمولی آشنا شویم. اکثر خطوط تلفن و تجهیزات مربوطه دارای محدودیت فرکانسی در ارتباط با سوئیچ، تلفن و سایر تجهیزاتی می باشند که بنوعی در فرآیند انتقال سیگنا ل ها دخالت دارند. صدای انسان (در یک مکالمه صوتی معمولی) توسط سیگنال هائی با فرکانس بین صفر تا ۳٤۰۰ قابل انتقال است. محدوده فوق بسیار ناچیز است (مثلا" اغلب بلندگوهای استریو که دارای محدوده بین ۲۰ تا ۲۰،۰۰۰ هرتز می باشند). کابل استفاده شده در سیستم تلفن قادر به انتقال سیگنال هائی با ظرفیت چندین میلیون هرتز می باشد. بدین ترتیب در مکالمات صوتی صرفا" از بخش بسیار محدودی از پهنای باند موجود، استفاده می گردد. با استفاده از پهنای باند استفاده نشده می توان علاوه بر بهره برداری از پتانسیل های موجود، بگونه ای عمل نمود که کیفیت مکالمات صوتی نیز دچار افت نگردند. تجهیزات پیشرفته ای که اطلاعات را بصورت دیجیتال ارسال می نمایند، قادر به استفاده از ظرفیت خطوط تلفن بصورت کامل می باشند. DSL چنین هدفی را دنبال می نماید.

در اغلب منازل و ادارات برخی از کشورهای دنیا، کاربران از یک DSL نامتقارن (ADSL) استفاده می نمایند. ADSL فرکانس های قابل دسترس دریک خط را تقسیم تا کاربران اینترنت قادر به دریافت و ارسال اطلاعات باشند. در مدل فوق، فرض بر این

گذاشته شده است که سرعت دریافت اطلاعات بمراتب بیشتر از سرعت ارسال اطلاعات باشد.

صوت و داده

کیفیت دریافت و ارسال اطلاعات از طریق DSL ، به مسافت موجود بین استفاده کننده و شرکت ارائه دهنده سرویس فوق بستگی دارد. ADSL از یک تکنولوژی با نام " تکنولوژی حساس به مسافت " استفاده می نماید. بموازات افزایش طول خط ارتباطی، کیفیت سیگنال افت و سرعت خط ارتباطی کاهش پیدا می نماید. ADSL دارای محدودیت ۱۸،۰۰۰ فوت (۵،٤٦۰ متر) است. کاربرانی که در مجاورت و نزدیکی شرکت ارائه دهنده سرویس DSL قرار دارند، دارای کیفیت و سرعت مناسبی بوده و بموازات افزایش مسافت ، کاربران اینترنت از نظر کیفیت و سرعت دچار افت خواهند شد. تکنولوژی ADSL قادر به ارائه بالاترین سرعت در حالت " **اینترنت به کاربر** " (Downstream) تا ۸ مگابیت در ثانیه است. (در چنین حالتی حداکثر مسافت ٦،۰۰۰ فوت و یا ۱،۸۲۰ متر خواهد بود). سرعت ارسال اطلاعات " از کاربر به اینترنت" (Upstream) دارای محدوده ٦٤۰ کیلوبیت در ثانیه خواهد بود. در عمل، بهترین سرعت ارائه شده برای ارسال اطلاعات از اینترنت به کاربر، ۱،۵ مگابیت در ثانیه و سرعت ارسال ارسال اطلاعات توسط کاربر بر روی اینترنت ، ٦٤۰ کیلوبیت در ثانیه است.

ممکن است این سوال در ذهن خوانندگان مطرح گردد که اگر تکنولوژی DSL دارای محدودیت فاصله است، چرا محدودیت فوق در رابطه با مکالمات صوتی صدق نمی کند؟ در پاسخ باید به وجود یک تقویت کننده کوچک که Loading coils نامیده می شود، اشاره کرد. شرکت های تلفن از تقویت کننده فوق، به منظور تقویت سیگنال صوتی استفاده می نمایند. متاسفانه تقویت کننده فوق با سیگنال های ADSL سازگار

نیست . لازم به ذکر است که سیگنال های ADSL ، در صورتیکه بخشی از خط ارتباطی از نوع فیبر نوری باشد، قادر به ارسال و دریافت اطلاعات نخواهند بود.

تقسیم سیگنال

از دو استاندارد متفاوت برای تقسیم سیگنالها (با یکدیگر سازگار نمی باشند)، استفاده می گردد. استاندارد ANSI برای ADSL سیستمی با نام **D**iscrete **Multitone** است. (DMT). اکثر تولیدکنندگان تجهیزات DSL از استاندارد فوق تبعیت می نمایند. استاندارد دیگری که نسبت به استاندارد DMT قدیمی تر و بسادگی پیاده سازی می گردد، استاندارد/**C**arrierless **A**mplitude **p**hase است(CAP). استاندارد CAP ، سیگنال ها را به سه باند مجزا تقسیم می نماید: مکالمات تلفن دارای باند صفر تا ٤ کیلو هرتز، کانال دریافت اطلاعات از کاربر برای سرویس دهنده دارای باندی بین ٢٥ تا ١٦٠ کیلو هرتز (Upstream) و کانال ارسال اطلاعات از سرویس دهنده برای کاربر، دارای محدوده ای که از ٢٤٠ کیلو هرتز شروع می گردد. حداکثر باند فوق به عوامل تفاوتی نظیر :طول خط ، تعداد کاربران موجود در یک شرکت تلفنی خاص و ...بستگی دارد، بهرحال حداکثر محدوده باند فوق از ١،٥ مگاهرتز تجاوز نخواهد کرد. سیستم CAP با استفاده از سه کانال فوق، قادر به ارسال سیگنال های مربوطه خواهد بود.

استاندارد DMT ، نیز سیگنال های مربوطه را به کانال های مجزا تقسیم می نماید.در استاندارد فوق از دو کانال مجزا برای ارسال و دریافت داده استفاده نمی گردد. DMT، داده را به ٢٤٧ کانال مجزا تقسیم می نماید.هر کانال دارای باند ٤ کیلو هرتز می باشند. (وضعیت فوق مشابه آن است که شرکت تلفن مربوطه ، خط مسی موجود را به ٢٤٧

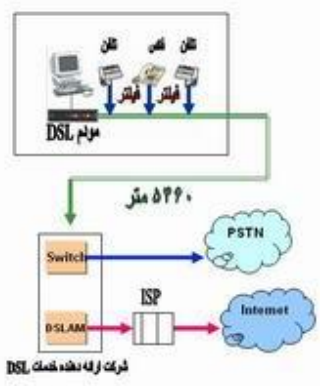
خط ٤ کیلو هرتزی مجزا تقسیم و هر یک از خطوط فوق را به یک مودم متصل نموده است. استفاده همزمان از ٢٤٧ مودم که هر یک دارای باند ٤ کیلوهرتز می باشند). هر یک از کانال ها، کنترل و در صورتیکه کیفیت یک کانال افت نماید، سیگنال بر روی کانال دیگر شیفت پیدا خواهد کرد. فرآیند شیفت دادن سیگنا ل ها بین کانال های متفاوت و جستجو برای یافتن بهترین کانال ، بصورت پیوسته انجام خواهد شد. برخی از کانال ها بصورت دو طرفه استفاده می شوند (ارسال و دریافت اطلاعات) کنترل و مرتب سازی اطلاعات در کانال های دو طرفه و نگهداری کیفیت هر یک از ٢٤٧ کانال موجود، پیاده سازی استاندارد DMT را نسبت به CAP بمراتب پیچیده تر نموده است. استاندارد DMT دارای انعطاف بمراتب بیشتری در رابطه با کیفیت خطوط و کانال ها ی مربوطه است .

استانداردهای CAP و DMT از دید کاربر دارای یک شباهت می باشند. در هر دو حالت از یک فیلتر به منظور فیلتر نمودن سیگنال های مربوطه استفاده می گردد. فیلترهای فوق از نوع Low-Pass می باشند. فیلترهای فوق دارای ساختاری ساده بوده و تمام سیگنال های بالاتر از یک محدوده را بلاک خواهند کرد. مکالمات صوتی در محدوده پایین تر از ٤ کیلو هرتز انجام می گیرند، بنابراین فیلترهای فوق تمام سیگنا ل های بالاتر از محدوده فوق را بلاک خواهند کرد. بدین ترتیب از تداخل سیگنال های داده با مکالمات تلفنی جلوگیری بعمل می آید.

تجهیزات DSL

ADSL از دو دستگاه خاص استفاده می نماید. یکی از دستگاهها در محل مشترکین و دستگاه دیگر برای ISP ، شرکت تلفن و یا سازمانهای ارائه دهنده خدمات DSL ، نصب می گردد. در محل مشترکین از یک ترانسیور DSL استفاده می گردد. شرکت ارائه دهنده خدمات DSL از یک DSL Access Multiplexer استفاده می نماید

(DSLAM). از دستگاه فوق به منظور دریافت اتصالات مشترکین استفاده می گردد. در ادامه به تشریح هر یک از دستگاههای فوق خواهیم پرداخت.



ترانسیور DSL

اکثر مشترکین DSL ، ترانسیور DSL را مودم DSL می نامند. مهندسین و کارشناسان شرکت های تلفن به دستگاه فوق ATU-R می گویند. صرفنظر از هر نامی که برای آن استفاده می شود، دستگاه فوق نقطه برقراری ارتباط بین کامپیوتر کاربر و یا شبکه به خط DSL است. ترانسیور با استفاده از روش های متفاوت به دستگاه مشترکین متصل می گردد. متداولترین روش، استفاده از اتصالات USB و یا اترنت است.

DSLAM

دستگاه فوق در مراکز ارائه دهنده سرویس DSL نصب و امکان ارائه خدمات مبتنی بر DSL را فراهم می نماید. DSLAM اتصالات مربوط به تعدادی از مشترکین را گرفته و آنها را به یک اتصال با ظرفیت بالا برای ارسال بر روی اینترنت تبدیل می نماید. دستگاههای DSLAM دارای انعطاف لازم در خصوص استفاده از خطوط DSL متفاوت ، پروتکل های متفاوت و مدولاسیون متفاوت (Cap,DMT) می باشند. در برخی از مدل های فوق امکان انجام عملیات خاصی نظیر اختصاص پویای آدرس های IP به مشترکین، نیز وجود دارد.

یکی از تفاوت های مهم بین ADSL و مودم های کابلی، نحوه برخورد و رفتار DSLAM است. کاربران مودم های کابلی از یک شبکه بسته بصورت اشتراکی استفاده

می نمایند. در چنین مواردیکه همزمان با افزایش تعداد کاربران ، کارآئی آنها تنزل پیدا خواهد کرد. ADSL برای هر یک از کاربران یک ارتباط اختصاصی ایجاد و آن را به DSLAM متصل می نماید. بدین ترتیب همزمان با افزایش کاربران، کارآئی مربوطه تنزل پیدا نخواهد کرد. وضعیت فوق تا زمانیکه کاربران از تمام ظرفیت موجود خط ارتباطی با اینترنت استفاده نکرده باشند، ادامه خواهد یافت. در صورت استفاده از تمام ظرفیت خط ارتباطی اینترنت، مراکز ارائه دهنده سرویس DSL می توانند نسبت به ارتقاء خط ارتباطی اینترنت اقدام تا تمام مشترکین متصل شده به DSLAM دارای کارآئی مطلوب در زمینه استفاده از اینترنت گردند.

آینده DSL

ADSL با سایر تکنولوژی های مربوط به دستیابی به اینترنت نظیر مودم های کابلی و اینترنت ماهواره ای رقابت می نماید. بر طبق آمار اخذ شده در سال ۱۹۹۹، بیش از ۳۳۰،۰۰۰ منزل در امریکا از DSL استفاده کرده اند. تعداد کاربران استفاده از مودم هـای کابلی تا سال ۱۹۹۹ به مرز ۱،۳۵۰،۰۰۰ کاربر رسیده است. بر اساس پیش بینی بعمل آمده تا اواخر سال ۲۰۰۳، تـعداد مـشترکین مودم های کابـلی به مرز ۸،۹۸۰،۰۰۰ و مشترکین DSL به ۹،۳۰۰،۰۰۰ خواهد رسید.

سرعت ADSL در حال حاضر حداکثر ۱،۵ مگابیت در ثانیه است. از لحاظ تئوری رسیدن به مرز ۷ مگابایت در ثانیه دور از دسترس نمی باشد. در این زمینه تحقیقات عمده ای صورت گرفته و تکنولوژی VDSL مطرح شده است.

VDSL

استفاده از خطوط با سرعت بالا به منظور دستیابی به اینترنت طی سالیان اخیر بشدت رشد داشته است. مودم های کابلی و خطوط ADSL دو رویکرد متفاوت در این زمینه می باشند. تکنولوژی های فوق امکان دستیابی کاربران را با سرعت مطلوب به اینترنت فراهم می نمایند. اینترنت بسرعت در حال رشد در تمامی ابعاد است. تلویزیون های دیجیتالی و پخش تصاویر ویدئویی دو کاربرد جدید در اینترنت بوده که علاقه مندان و مشتاقان زیادی را به خود جلب نموده است. به منظور ارائه خدمات فوق و سایر خدمات مشابه، کاربران و استفاده کنندگان اینترنت نیازمند استفاده از خطوط بمراتب سریعتر نسبت به وضعیت فعلی می باشند. مودم های کابلی و یا خطوط ADSL علیرغم ارائه سرعت مناسب در کاربـردهائی که به آنها اشـــاره گردید، فاقد سرعت لازم می باشند.

اخیرا" سازمانها و شرکت های متعددی تکنولوژی **VDSL** (Very high bit-rate DSL) را مطرح نموده اند. برخی از شرکت ها اقدام به ارائه سرویس فوق در برخی از نقاط کشورامریکا نموده اند. VDSL پهنای باند بسیار بالائی را ارائه و سرعت انتقال اطلاعات ۵۲ مگابیت در ثانیه است . سرعت فوق در مقایسه با DSL (حداکثر سرعت ۸ تا ده مگابیت در ثانیه) و یا مودم های کابلی بسیار بالا بوده و قطعا" نقطه عطفی در زمینه دستیابی به اینترنت از نظر سرعت خواهد بود. نقطه عطف قبلی، گذر از مرحله استفاده از مودم های با ظرفیت ۵۶ کیلو بیت در ثانیه به broadband بود.

ADSL از دو دستگاه خاص استفاده می نماید. یکی از دستگاهها در محل مشترکین و دستگاه دیگر برای ISP، شرکت تلفن و یا سازمانهای ارائه دهنده خدماتDSL، نصب می گردد. در محل مشترکین از یک ترانسیور DSL استفاده می گردد. شرکت ارائه دهنده خدمات DSL از یک Multiplexer DSL Access استفاده می نماید (DSLAM) . از دستگاه فوق به منظور دریافت اتصالات مشترکین استفاده می گردد.

اکثر مشترکین DSL، ترانسیور DSL را مودم DSL می نامند. مهندسین و کارشناسان شرکت های تلفن به دستگاه فوق ATU-R می گویند. صرفنظر از هر نامی که برای آن استفاده می شود، دستگاه فوق نقطه برقراری ارتباط بین کامپیوتر کاربر و یا شبکه به خط DSL است. ترانسیور با استفاده از روش های متفاوت به دستگاه مشترکین متصل می گردد. متداولترین روش، استفاده از اتصالات USB و یا اترنت است.

دستگاه فوق در مراکز ارائه دهنده سرویس DSL نصب و امکان ارائه خدمات مبتنی بر DSL را فراهم می نماید. DSLAM اتصالات مربوط به تعدادی از مشترکین را گرفته و آنها را به یک اتصال با ظرفیت بالا برای ارسال بر روی اینترنت تبدیل می نماید.

دستگاههای DSLAM دارای انعطاف لازم در خصوص استفاده از خطوط DSL متفاوت، پروتکل های متفاوت و مدولاسیون متفاوت (Cap,DMT) می باشند. در برخی از مدل های فوق امکان انجام عملیات خاصی نظیر اختصاص پویای آدرس های IP به مشترکین، نیز وجود دارد.

یکی از تفاوت های مهم بین ADSL و مودم های کابلی، نحوه برخورد و رفتار DSLAM است. کاربران مودم های کابلی از یک شبکه بسته بصورت اشتراکی استفاده می نمایند. در چنین مواردیکه همزمان با افزایش تعداد کاربران، کارآئی آنها تنزل پیدا خواهد کرد. ADSL برای هر یک از کاربران یک ارتباط اختصاصی ایجاد و آن را به DSLAM متصل می نماید. بدین ترتیب همزمان با افزایش کاربران، کارآئی مربوطه تنزل پیدا نخواهد کرد. وضعیت فوق تا زمانیکه کاربران از تمام ظرفیت موجود خط ارتباطی با اینترنت استفاده نکرده باشند، ادامه خواهد یافت. در صورت استفاده از تمام ظرفیت خط ارتباطی اینترنت، مراکز ارائه دهنده سرویس DSL می توانند نسبت به ارتقاء خط ارتباطی اینترنت اقدام تا تمام مشترکین متصل شده به DSLAM دارای کارآئی مطلوب در زمینه استفاده از اینترنت گردند.

سرعت VDSL

عملکرد VDSL ، در اغلب موارد مشابه ADSL است . علیرغم شباهت های موجود در این زمینه اختلافات متعددی نیز وجود دارد. VDSL قادر به ارائه سرعت ۵۲ مگابیت در ثانیه برای ارسال اطلاعات از اینترنت به کاربر (Downstream) و ۱۶ مگابیت در ثانیه برای ارسال اطلاعات کاربر بر روی اینترنت (Upstream) است.

سرعت های فوق بمراتب بیشتر از ADSL است. در ADSL حداکثر سرعت ارسال اطلاعات از اینترنت به کاربر، ۸ مگابیت در ثانیه و سرعت ارسال اطلاعات از کاربر به اینترنت ۸۰۰ کیلوبیت در ثانیه است. VDSL سرعت بالای خود را مدیون محدودتر شدن فاصله بین مشترکین و مرکز ارائه دهنده سرویس فوق است . حداکثر مسافت موجود ٤،۰۰۰ فوت (۱،۲۰۰ متر) است.

شرکت های تلفن در حال جایگزین نمودن اغلب تجهیزات (مربوط به تغذیه اطلاعات) به فیبر نوری می باشند. اکثر شرکت های تلفن از تکنولوژی FTTC (Fiber to the curb) استفاده می نمایند. شرکت های فوق قصد دارند که تمام خطوط مسی موجود را تا محلی که از آنها انشعاب گرفته شده و به منازل مشترکین توزیع می گردد، تعویض نمایند. شرکت های تلفن در تلاش برای پیاده سازی سیستم Fiber To the Neighborhood(FFTN) می باشند. در روش فوق در عوض نصب کابل فیبر نوری در هرخیابان ، FFTN دارای فیبر مورد نظر تا جعبه اتصالات (انشعابات) برای یک همسایه (مشترک) خاص است.

با ااستقرار یک ترانسیور VDSL در منزل و یک VDSL gateway در جعبه تقسیم اتصالات، محدودیت فاصله کم رنگ خواهد شد. gateway باعث مراقبت از تبدیلات آنالوگ به دیجیتال و دیجیتال به آنالوگ که باعث غیرفعال شدن ADSL بر روی خطوط فیبر نوری می گردد. Gateway داده های ورودی و دریافت شده از ترانسیور را به پالس های نور تبدیل تا زمینه ارسال آنها از طریق فیبر نوری فراهم گردد. زمانیکه داده ها برای کامپیوتر کاربر ارسال می گردند(برگشت داده)، Gateway موجود سیگنال های

ورودی از فیبر نوری را تبدیل و آنها را برای ترانسیور کاربر ارسال می نماید. فرآیند فوق در هر ثانیه میلیون ها مرتبه تکرار خواهد گردید.

ADSL و VDSL صرفا" دو نمونه از تکنولوژط های مربوط به DSL spectrum می باشند . در ادامه به بررسی سایر مدل های مربوط به تکنولوژی فوق اشاره خواهد شد.

مقایسه انواع DSL

نمونه های متفاوتی از تکنولوژی DSL تاکنون پیاده سازی شده است:

- ADSL(Asymmetric DSL). درمدل فوق بدلیل تفاوت سرعت دریافت و ارسال اطلاعات از واژه " نامتقارن " استفاده شده است. ماهیت عملیات انجام شده توسط کاربران اینترنت بگونه ای است که همواره حجم اطلاعات دریافتی بمراتب بیشتر از اطلاعات ارسالی است.
- HDSL(High bit-rate DSL) . سرعت مدل فوق در حد خطوط T1 است (۵/۱ مگابیت در ثانیه) .سرعت دریافت و ارسال اطلاعا ت در روش فوق یکسان بوده و به منظور ارائه خدمات نیاز به دو خط مجزا نسبت به خط تلفن معمولی موجود است.
- ISDL(ISDN DSL) . مدل فوق در ابتدا در اختیار کاربران استفاده کننده از ISDN قرار گرفت. ISDL در مقایسه با سایر مدل های DSL دارای پایین ترین سرعت است . سرعت این خطوط ١٤٤ کیلوبیت در ثانیه است (دو جهت).
- MSDSL(Multirate Symmetric DSL) . در مدل فوق سرعت ارسال و دریافت اطلاعات یکسان است . نرخ سرعت انتقال اطلاعات توسط مرکز ارائه دهنده سرویس DSL ، تنظیم می گردد.
- RADSL(Rate Adaptive) . متداولترین مدل ADSL بوده و این امکان را به مودم خواهد داد که سرعت برقراری ارتباط را با توجه به عواملی نظیر مسافت و کیفیت خط تعیین نماید.

- **SDLS**(Symmetric DSL) . سرعت ارسال و دریافت اطلاعات یکسان است . در مدل فوق بر خلاف HDSL که از دو خط مجزا استفاده می نماید، صرفا" به یک خط نیاز خواهد بود.
- **VDSL**(Very high bit-rate) . مدل فوق بصورت "نامتقارن " بوده و در مسافت های کوتاه بهمراه خطوط مسی تلفن استفاده می گردد.
- **VoDSL**(Voice-over DSL). یک نوع خاص از IP تلفنی است . در مدل فوق چندین خط تلفن ترکیب و به یک خط تلفن تبدیل تبدیل می شوند.

جدول زیر نمونه های متفاوت تکنولوژی DSL را نشان می دهد.

نوع DSL	حداکثر سرعت ارسال	حداکثر سرعت دریافت	حداکثر مسافت	خطوط مورد نیاز	امکان استفاده از تلفن
ADSL	800 Kbps	8 Mbps	18,000 ft (5,500 m)	1	Yes
HDSL	1.54 Mbps	1.54 Mbps	12,000 ft (3,650 m)	2	No
IDSL	144 Kbps	144 Kbps	35,000 ft (10,700 m)	1	No
MSDSL	2 Mbps	2 Mbps	29,000 ft (8,800 m)	1	No
RADSL	1 Mbps	7 Mbps	18,000 ft (5,500 m)	1	Yes
SDSL	2.3 Mbps	2.3 Mbps	22,000 ft (6,700 m)	1	No
VDSL	16 Mbps	52 Mbps	4,000 ft (1,200 m)	1	Yes

اینترنت ماهواره ای

کاربران اینترنت با استفاده از امکانات متعددی قادر به اتصال به اینترنت و استفاده از منابع موجود می باشند. استفاده از خطوط تلفن معمولی، مودم کابلی، خطوط DSL، اینترنت بدون کابل، نمونه هائی در این زمینه می باشند. در صورتیکه کاربران اینترنت قادر به استفاده از هیچکدام از وسایل ارتباطی فوق نباشند (بدلیل وجود مسافت زیاد بین استفاده کننده و مرکز ارائه دهنده خدمات مورد نظر)، امکان استفاده از اینترنت ماهواره ای وجود خواهد داشت. اینترنت ماهواره ای از خطوط تلفن و یا سیستم های مبتنی بر کابل برای برقراری ارتباط استفاده نمی نماید. در این نوع سیستم ها از یک "بشقاب ماهواره ای " برای ارسال و دریافت اطلاعات (دو طرفه) استفاده می گردد. معمولا" در این نوع سیستم ها سرعت ارسال اطلاعات معادل یک دهم سرعت دریافت اطلاعات است. مودم های کابلی و خطوط DSL نسبت به اینترنت ماهواره ای دارای سرعت بمراتب بیشتری در رابطه با دریافت اطلاعات می باشند. سرعت اینترنت ماهواره ای ده برابر سرعت یک مودم معمولی است.

موسسات و شرکت های متفاوتی تاکنون سرویس اینترنت ماهواره ای را در اختیار علاقه مندان قرار می دهند. Teledesic، StarBand,Pegasus Express و Tachyon نمونه هائی از شرکت های ارائه دهنده خدمات اینترنت ماهواره ای بصورت دو طرفه می باشند. سرویس ارائه شده توسط Tachyon در امریکا، اروپای غربی و مکزیک ارائه شده است . Pegasus Express نسخه دو طرفه DirectPC است.

در اینترنت ماهواره ای دو طرفه از عناصر زیر استفاده می شود :

- یک "بشقاب " (Dish) با ابعاد دو و یا سه فوت
- دو عدد مودم (Uplink,downlink)
- کابل های کواکسیال بین بشقاب و مودم

در اینترنت ماهواره ای دو طرفه از تکنولوژی IP multicasting استفاده می شود. در این حالت امکان ارتباط ۵،۰۰۰ کانال بصورت همزمان و از طریق صرفا" یک ماهواره فراهم خواهد شد. IP multicasting ، داده های مورد نظر را از یک نقطه به چندین نقطه و بصورت فشرده، ارسال خواهد کرد(در یک زمان). با فشرده سازی اطلاعات، حجم داده ها کاهش و از پهنای باند موجود استفاده بهینه خواهد شد.

در سیستم DirectPC (ارائه شده توسط DirectTV) ، کاربران همچنان می بایست از یک ISP استفاده نمایند. در این حالت کاربران برای ارسال اطلاعات در ابتدا می بایست با ISP تماس و در ادامه اقدام به ارسال و یا دریافت اطلاعات نمایند.

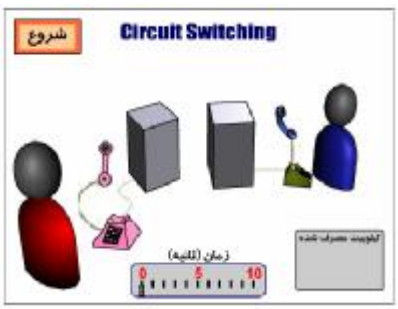
VOIP

IP تلفنی، ارسال مکالمات تلفـــنی بر روی یک شبـکه مبتنی بر داده است. به نکنولوژی فوق Voice-over IP(VoIP) نیز گفته می شود. امروزه مکالمات گسترده ای از طریق شبکه های مبتنی بر داده (نظیر اینترنت) انجام می شود.

Circuit Switching

شرکت های تلفن بیش از یکصد سال است که از تکـــنولوژی Circuit Switching استفاده می نمایند. در روش فوق بمحض برقراری ارتبـــاط بین دو نفر، در تمام مدت زمان مکالمه یک مدار اختصاصی برای آنها در نظر گرفته خواهد شد. بدین ترتیب برای دو نقطه مربوطه یک ارتباط دو سویه ایجاد می گردد. نحوه انجام یک مکالمه صوتی به صورت زیر است:

- پس از برداشتن گوشی تلفن یک بوق شنیده می گردد. بوق فوق بمنزله برقراری ارتباط با شرکت تلفن (مرکز مربوطه) است.
- با استفاده از سیستم تلفن ، اقدام به شماره گیری می گردد.
- ارتباط مورد نظر از طریق مجموعه ای از سوئیچ ها عبور داده شده تا به مخاطب مورد نظر برسد.
- یک ارتباط بین تلفن شما و مخاطب برقرار و یک مدار فعال می گردد.
- مکالمه با مخاطب مورد نظر در مدت زمان دلخواه انجام می گیرد.
- پس از قطع مکالمه ، مدار فعال شده بین شما و مخاطب غیر فعال خواهد شد.



فرض کنید مدت زمان مکالمه شما ده دقیقه باشد ، در طول مدت زمان فوق مدار ایجاد شده بین دو تلفن بصورت پیوسته فعال خواهد بود. در سیستم های قدیمی مخابراتی، مکالمه تلفنی با نرخ انتقال اطلاعات ثابت ٦٤ کیلو بیت در ثانیه و یا ١٠٢٤ بیت در ثانیه در هر جهت انجام می گرفت (مجموع نرخ انتقال اطلاعات ١٢٨ کیلوبیت در ثانیه) .با توجه به اینکه در هر کیلوبایت، هشت کیلوبیت وجود دارد ، بنابراین در هر ثانیه ١٦ کیلو بایت و یا در هر دقیقه ٩٦٠ کیلوبایت اطلاعات ارسال می گردد(زمانی که مدار فعال است) .بنابراین در مدت زمان ده دقیقه ارتباط تلفنی ، مجموع اطلاعات ارسال شده ٩٦٠٠ کیلو بایت (٩/٤ مگابایت) خواهد بود.

در یک مکالمه تلفنی اکثر داده های ارسال شده بیهوده می باشند. زمانی که شما حرف می زنید، مخاطب صرفا" گوش می دهد. این بدان معنی است که در هر مقطع زمانی، ازنصف خط ارتباطی بیشتر استفاده نمی گردد. (سکوت موجود بر روی خط در مدت زمان برقراری ارتباط زیاد خواهد بود) در این حالت حجم اطلاعـــــات ارسال شده، به ٤/٧ مگابایت تنزل پیدا خواهد کرد.

شبکه های مبتنی بر داده از روش Circuit switching استفاده نکرده و در مقابل، روش Packet Switching استفاده می گردد.

Packet Switching

در روش Packet Switching بر خلاف Switching Circuit که بصورت پیوسته ارتباط را فعال نگه می دارد، صرفا" در زمان ارسال اطلاعات (یک بخش کوچک داده که به آن packet گفته می شود) ارتباط فعال خواهد شد. اطلاعات مربوط به فرستنده به مجموعه ای از Packet تقسیم می گردد. در هر یک از بسته های اطلاعاتی آدرس فرستنده و دریافت کننده اطلاعات قرار خواهد گرفت. دریافت کننده بسته های اطلاعاتی، اطلاعات را به یکدیگر ملحق تا اطلاعات اولیه بوجود آیند.

روش فوق بسیار کارآ بوده و زمان فعال بودن ارتباط بین فرستنده و گیرنده را به حداقل مقدار خود می رساند. بدین ترتیب ترافیک موجود بر روی شبکه نیز کاهش خواهد یافت . کامپیوترهای فرستنده و گیرنده در زمان ارتباط با یکدیگر قادر به دریافت و یا ارسال اطلاعات برای سایر کامپیوترها نیز خواهند بود.

تکنولوژی VoIP از روش Packet Switching استفاده می کند. بااستفاده از روش فوق امکان برقراری چندین مکالمه تلفنی فراهم می گردد. با استفاده از PSTN ، یک مکالمه ده دقیقه ای ، ده دقیقه کامل از زمان انتقال با نرخ ۱۲۸ کیلوبیت در ثانیه را اشغال خواهد کرد. در روش VoIP ، مکالمه ده دقیقه ای اشاره شده صرفا" ۵/۳ دقیقه زمان انتقال را با نرخ ٦٤ کیلوبیت در ثانیه اشغال خواهد کرد. در این حالت ٦٤ کیلوبیت در ثانیه برای مدت ۵/۳ دقیقه ، و ۱۲۸ کیلوبیت در ثانیه برای زمان باقیمانده ۵ /٦ آزاد خواهد ماند.

فرض کنید که شرکت شما دستگاه مورد نظر بمنظور استفاده از سرویس VoIP را خریداری و نصب کرده باشد. در شرکت مربوطه صدها تلفن و یک PBX) Private branch exchange) نیز نصب شده است . PBX سوئیچی است که از آن بمنظور ارتباط مجموعه ای از تلفن ها به یکدیگر و به یک یا چندین خط خارج از شرکت استفاده می گردد. در مثال فوق PBX بصورت یک gateway است.

از gateway بمنظور ارتباط دستگاههای موجود در دو شبکه متفاوت استفاده میگردد. PBX یک Gateway است .(چون سیگنال های استاندارد circuit-switching هر یک از تلفن ها را به داده های دیجیتال بمنظور ارسال از طریق یک شبکه مبتنی بر IP و Packet Switching تبدیل می نماید).

روش برقراری یک مکالمه از طریق یک شبکه Packet-Switching و با استفاده از VoIP بصورت زیر است :

- دریافت کننده را فعال تا از طریق آن یک سیگنال برای PBX ارسال گردد.
- PBX سیگنال را دریافت و یک بوق آزاد را برای فرستنده ارسال می دارد.

- فرستنده اقدام به شماره گیری تلفن مخاطب مورد نظر را می نماید. شماره فوق در ادامه توسط PBX بصورت موقت ذخیره می گردد.
- پس از مشخص نمودن شماره توسط فرستنده، PBX بمنظور اطمینان از صحت فرمت، آن را بررسی خواهد کرد.
- PBX در رابطه با نحوه تطبیق شماره دریافتی با شخص مورد نظر اقدامات لازم را انجام خواهد داد. درفرآیند تطبیق، شماره مورد نظر به آدرس IP دستگاه دیگر که "میزبان IP" نامیده می گردد، ملحق می گردد. "میزبان IP" عملا" یک PBX دیجیتالی دیگر است که به سیتم تلفن محلی که با آن ارتباط برقرار شده ، نصب شده است. در موارد خاصی که مخاطب از یک سرویس گیرنده VoIP مبتنی بر کامپیوتر استفاده می نماید ، "میزبان IP" ، سیستمی است که قصد برقراری ارتباط با آن وجود دارد.
- یک session بین PBX اداره تماس گیرنده و "میزبان IP" برقرار می گردد. هر سیستم می بایست از پروتکل های یمشابه بمنظور برقراری ارتباط استفاده نماید. سیستم ها دو کانال برای هر جهت را پیاده سازی خواهند کرد.
- مکالمه به مدت زمان مورد نظر انجام می گیرد.در زمان برقراری مکالمه، PBX شرکت شما و میزبان IP مخاطب، بسته های اطلاعاتی را ارسال و یا دریافت می دارند.
- مکالمه به اتمام رسیده و دریافت کننده غیرفعال می گردد.
- پس از قطع ارتباط ، مدار(ارتباط) موجود بین تلفن تماس گیرنده و PBX آزاد می گردد.
- PBX سیگنالی را برای میزبان IP ارسال و خاتمه مکالمه را اعلام می نماید.
- پس از اتمام session ، دستگاه PBX شماره تلفن تطبیق داده شده به "میزبان IP" را از حافظه خود پاک می نماید.

بمنظور برقراری ارتباط از طریق تلفن با دستگاههائی نظیر: کامپیوتر در طول یک شبکه، می بایست از یک پروتکل مشترک استفاده گردد.

پروتکل

از دو پروتکل عمده برای VoIP استفاده می شود. پروتکل های فوق روش های مربوط به ارتباط دستگاههای متفاوت از طریق VoIP را مشخص و Codec های صوتی را نیز تعیین می نماید. "کدک " از تلفیق دو واژه **Code** و **Decode** تشکیل شده است. کدک ، یک سیگنال صوتی را به یک سیگنال دیجیتالی فشرده شده تبدیل می نماید. اولین پروتکل H.323 است. پروتکل فوق استاندارد ارائه شده توسط ITU(International Telecommunication Union) است. H.323 یک پروتکل پیشرفته و پیچیده است. پروتکل فوق مشخصات لازم برای ویدئوکنفرانس های محاوره ای و اشتراک داده و نرم افزارهای صوتی نظیر IP تلفنی را تعریف می نماید. H.323 دارای مجموعه ای از سایر پروتکل ها بوده که هر یک دارای کاربرد خاص خود می باشند.

H.323 Protocol			
Transport	Data	Audio	Video
H.225 H.235 H.245 H.450.1 H.450.2 H.450.3 RTP X.224.0	T.122 T.124 T.125 T.126 T.127	G.711 G.722 G.723.1 G.728 G.729	H.261 H.263

خیراً پروتکل دیگری با نام **SIP**(session Initiation Protocol) توسط IETF ارائه شده است.SIP نسبت به H.323 دارای کارائی بمراتب بیشتری بوده و صرفاً برای IP تلفنی طراحی و پیاده سازی شده است.

روش های استفاده از VoIP

برای استفاده از VoIP ، چهار حالت متفاوت وجود دارد:

- **کامپیوتر به کامپیوتر** . ساده ترین روش استفاده از VoIP است. شرکت های متعددی، خدمات فوق را ارائه می دهند. برای استفاده از روش فوق به نرم افزار مربوطه، میکروفن، بلندگو، کارت صدا و خط ارتباطی با سرعت مناسب (خطوط DSL و یا مودم های کابلی) نیاز خواهد بود. MSN Explorer یک نمونه از نرم افزارهای مربوطه در این زمینه است.
- **کامپیوتر به تلفن** . با استفاده از روش فوق می توان از طریق کامپیوتر با هر شخص که دارای یک خط تلفن است، ارتباط برقرار کرد. برای استفاده از روش فوق به یک نرم افزار سرویس گیرنده نیاز خواهد بود. نرم افزار فوق اغلب بصورت رایگان در اختیار علاقه مندان قرار می گیرد. هزینه مکالمات انجام شده، بمراتب پایین تر از روش های قدیمی است.
- **تلفن به کامپیوتر** . برخی از شرکت ها ، شماره تلفن های خاصی را بمنظور تماس کاربران معمولی تلفن با کاربران کامپیوتر فراهم نموده اند. نصب یک نرم افزار خاص بمنظور انجام عملیات فوق، بر روی کامپیوتر سرویس گیرندگان، الزامی است.
- **تلفن به تلفن** . با استفاده از Gateways می توان با هر تلفن استاندارد در سطح دنیا ارتباط برقرار کرد. برای استفاده از سرویس فوق که توسط برخی از شرکت ها ارائه می گردد، می بایست در ابتدا با یکی از Gateway های مربوط به آنان تماس برقرار کرد. در ادامه شماره تلفن مورد نظر خود را مشخص و نهایتاً توسط

شرکت مربوطه امکان برقراری ارتباط با استفاده از یک شبکه مبتنی بر IP فراهم خواهد شد. در این روش، لازم است که در ابتدا از یک شماره خاص استفاده گردد.(شماره مربوط به Gateway شرکت ارائه دهنده خدمات فوق).

اکثر سازمانها و موسسات با نصب سیستم های VoIP امکان استفاده از IP تلفنی را برای کاربران خود فراهم نموده اند. تکنولوژی فوق با سرعت در حال رشد و گسترش همگانی است. کیفیت بالا و هزینه پایین از مهمترین دلایل فراگیر شدن تکنولوژی فوق است.

تجارت الکترونیکی

تجارت الکترونیکی در سالیان اخیر با استقبال گسترده جوامع بشری روبرو شده است. امروزه کمتر شخصی را می توان یافت که واژه فوق برای او بیگانه باشد. نشریات، رادیو و تلویزیون به صورت روزانه موضوعاتی در رابطه با تجارت الکترونیکی را منتشر و افراد و کارشناسان از زوایای متفاوت به بررسی مقوله فوق می پردازند. شرکت ها و موسسات ارائه دهنده کالا و یا خدمات همگام با سیر تحولات جهاتی در زمینه تجارت الکترونیکی در تلاش برای تغییر ساختار منطقی و فیزیکی سازمان خود در این زمینه می باشند.

تجارت

قبل از بررسی " تجارت الکترونیکی "، لازم است در ابتدا یک تصویر ذهنی مناسب از تجارت سنتی را ارائه نمائیم . در صورت شناخت " تجارت "، با " تجارت الکترونیکی " نیز آشنا خواهیم شد.

برای واژه "تجارت" در اکثر واژه نامه ها تعاریف زیر ارائه شده است:

- مبادلات اجتماعی: تبادل ایده ها ، عقاید و تمایلات (خواسته ها)
- مبادله یا خرید و فروش کالا در مقیاس بالا که به همراه حمل کالا از نقطه ای به نقطه ای دیگر می باشد .

در ادامه ، تعریف دوم ارائه شده برای "تجارت " را به عنوان محور بحث انتخاب و بر روی آن متمرکز خواهیم شد.

تجارت در ساده ترین نگاه، مبادله کالا و خدمات به منظور کسب درآمد (پول) است. زندگی انسان مملو از فرآیندهای تجاری بوده و تجارت با میلیونها شکل متفاوت در زندگی بشریت نمود پیدا کرده است . زمانیکه کالای مورد نظر خود را از یک فروشگاه تامین و خریداری می نمائید، در تجارت شریک و در فرآیندهای آن درگیر شده اید. در صورتیکه در شرکتی مشغول بکار هستید که کالائی را تولید می نماید ، درگیر یکی دیگر

از زنجیره های تجارت شده اید. تمام جلوه های تجارت با هر رویکرد و سیاستی دارای خصایص زیر می باشند:

- **خریداران** . افرادیکه با استفاده از پول خود قصد خرید یک کالا و یا خدمات را دارند.
- **فروشندگان** . افرادیکه کالا و خدمات مورد نیاز خریداران را ارائه می دهند. فروشندگان به دو گروع عمده تقسیم می گردند: خرده فروشان، که کالا و یا خدماتی را مستقیما" در اختیار متقاضیان قرار داده و عمده فروشان و عوامل فروش، که کالا و خدمات خود را در اختیار خرده فروشان و سایر موسسات تجاری می نمایند.
- **تولیدکنندگان** . افرادیکه کالا و یا خدماتی را ایجاد تا فروشندگان آنها را در اختیار خریداران قرار دهند. یک تولید کننده با توجه به ماهیت کار خود همواره یک فروشنده نیز خواهد بود. تولیدکنندگان کالای تولیدی خود را به عمده فروشان ، خرده فروشان و یا مستقیما" به مصرف کننده گان می فروشند.

همانگونه که مشاهده می گردد ، "تجارت " از زاویه فوق دارای مفاهیم ساده ای است. تجارت از خرید یک محصول ساده نظیر " بستنی " تا موارد پیچیده ای نظیر اجاره ماهواره را شامل می گردد. تمام جلوه های تجارت از ساده ترین سطح تا پیچیده ترین حالت آن ، بر مقولاتی همچون : خریداران ، فروشندگان و تولیدکنندگان متمرکز خواهد بود.

عناصر تجارت

زمانیکه قصد معرفی عناصر ذیربط در تجارت و فعالیت های تجاری وجود داشته باشد، موضوعات و موارد مورد نظر بدلیل درگیر شدن با جزئیات پیچیده تر بنظر خواهند آمد. عناصر ذیل تمام المان های ذیربط در یک فعالیت تجاری معمولی را تشریح می نماید. در این حالت ، فعالیت شامل فروش برخی محصولات توسط یک خرده فروش به مصرف کننده است :

- در صورت تمایل فروش محصول و یا محصولاتی به یک مصرف کننده، مسئله اساسی داشتن کالا و یا خدماتی خاص برای عرضه است. کالا می تواند هر چیزی را شامل گردد. فروشنده، ممکن است کالای خود را مستقیما" از تولید کننده و یا از طریق یک عامل فروش تهیه کرده باشد. در برخی حالات ممکن است فروشنده ، خود کالائی را تولید و بفروش می رساند.
- فروشنده برای فروش کالا و یا خدمات می بایست " مکانی مناسب " را در اختیار داشته باشد. مکان مورد نظر می تواند در برخی حالات بسیار موقتی باشد. مثلا" یک شماره تلفن خود بمنزله یک مکان است. در چنین مواردی متقاضی کالا و یا خدمات با تماس تلفنی با فروشنده قادر به ثبت سفارش و دریافت کالای مورد نظر خود خواهد بود. برای اکثر کالاهای فیزیکی می بایست مکان ارائه کالا ، یک مغازه و یا فروشگاه باشد.
- برای فروش کالا و یا خدمات ، فروشندگان می بایست از راهکارهائی برای جذب افراد به مکان خود استفاده نمایند. فرآیند فوق " مارکتینگ " نامیده می شود. در صورتیکه افراد از محل و مکان ارائه یک کالا و خدمات آگاهی نداشته باشند، امکان فروش هیچگونه کالائی وجود نخواهد داشت. انتخاب محل ارائه کالا در یک مرکز تجاری شلوغ ، یکی از روش های افزایش تردد به مکان ارائه کالا است. ارسال پستی کاتولوگ ها ی مربوط به محصولات، یکی دیگر از روش های معرفی مکان ارائه یک کالا و یا خدمات است. استفاده از شیوه های متفاوت تبلیغاتی، راهکاری دیگر در معرفی مکان ارائه کالا است.
- فروشنده نیازمند روشی برای دریافت سفارشات است. استفاده از تلفن و نامه، نمونه هائی از روش های دریافت سفارش متقاضیان می باشد. حضور فیزیکی در مکان ارائه یک کالا و یا خدمات از دیگر روش های سنتی برای ثبت سفارش کالا است . پس از ثبت سفارش، فرآیندهای لازم توسط پرسنل شاغل در شرکت و یا موسسه ارائه دهنده کالا و یا خدمات انجام خواهد گرفت.

- فروشنده نیازمند روشی برای دریافت پول است. استفاده از چک، کارت اعتباری و یا پول نقد روش های موجود در این زمینه می باشند. در برخی از فعالیت های تجاری از فروشنده تا زمان توزیع کالا پولی دریافت نمی گردد.
- فروشنده نیازمند استفاده از روشی برای عرضه و توزیع کالا و یا خدمات می باشد. در برخی از سیستم ها بمحض انتخاب کالا توسط مشتری و پرداخت وجه آن، عملیات توزیع کالا بصورت اتوماتیک انجام خواهد شد. در سیستم های ثبت سفارش مبتنی بر نامه، کالای خریداری شده پس از بسته بندی به مقصد مشتری ارسال خواهد شد. در مواردیکه حجم کالا زیاد نباشد از مبادلات پستی به منظور ارسال کالا استفاده شده و در مواردیکه حجم کالا زیاد باشد از کامیون، قطار و یا کشتی برای ارسال و توزیع کالا استفاده می گردد.
- در برخی موارد ، خریداران یک کالا تمایل و علاقه ای نسبت به آن چیزی که خریداری نموده اند نداشته و قصد برگشت آن را دارند. فروشندگان کالا و یا خدمات می بایست از روش هائی برای قبول موارد "برگشت از فروش " استفاده نمایند.
- در برخی موارد ممکن است کالائی در زمان توزیع آسیب دیده باشد. فروشندگان می بایست از روش های برای تضمین گارانتی استفاده نمایند.
- برخی از کالاهای ارائه شده به مشتریان دارای پیچیدگی های خاص خود بوده و نیازمند استفاده از خدمات پس از فروش و یا حمایت فنی می باشند. در چنین مواردی وجود بخش هائی در شرکت و یا موسسه ارائه دهنده کالا و یا خدمات الزامی خواهد بود. کامپیوتر یکی از نمونه کالاهائی است که نیازمند خدمات پس از فروش و حمایت فنی از دیدگاه مشتریان (خریداران) خواهد بود.

تمام عناصر اشاره شده را می توان در یک شرکت تجاری سنتی مشاهده کرد. فعالیت های تجاری شرکت های فوق می تواند شامل مقوله های متفاوتی باشد.

در تجارت الکترونیکی تمام عناصر اشاره شده، حضوری مشهود با تغییرات خاصی دارند. به منظور مدیریت و اجرای تجارت الکترونیکی به عناصر زیر نیاز خواهد بود:

- یک محصول
- محلی برای فروش کالا. در تجارت الکترونیکی یک وب سایت بمنزله مکان ارائه کالا و یا خدمات خواهد بود.
- استفاده از روش و یا روش هائی برای مراجعه به سایت
- استفاده از روشی برای ثبت سفارش.(اغلب بصورت فرم ها ئی در نظر گرفته می شود)
- استفاده از روشی برای دریافت پول. (کارت اعتباری از نمونه های متداول است)
- استفاده از روشی برای توزیع کالا
- استفاده از روشی برای موارد برگشت داده شده توسط خریداران
- استفاده از روشی برای موارد مربوط به گارانتی
- استفاده از روشی برای ارائه خدمات پس از فروش (پست الکترونیکی ، ارائه پایگاه های اطلاع رسانی و...)

چرا تبلیغات زیاد ؟

پیرامون تجارت الکترونیکی تبلیغات زیاد و گاها" بی رویه ای انجام می گیرد. علت تبلیغات زیاد در رابطه با تجارت الکترونیکی را می توان با استناد به برخی از آمارها و ارقام موجود متوجه شد:

- تا سال ۲۰۰۱ میلادی بالغ بر ۱۷ میلیارد دلار در سطح خرده فروشی مبادلات تجاری صورت گرفته است.
- تعداد استفاده کنندگان از تجارت الکترونیکی از رقم ۱،۳ میلیون نفر در سال ۱۹۹٦ به ۸ میلیون نفر در سال ۲۰۰۱ رسیده است.

- ۷۰ درصد کاربران و استفاده کنندگان از کامپیوتر در منزل به اینترنت متصل و این گروه ٦۰ درصد خرید از طریق اینترنت را انجام داده اند.

بر اساس آمارهای موجود، گروه کالاهای زیر دارای بیشترین میزان فروش تجارت الکترونیکی را بخود اختصاص داده اند:

- محصولات کامپیوتری (نرم افزار، سخت افزار)
- کتاب
- خدمات مالی
- سرگرمی ها
- موزیک
- الکترونیک های خانگی
- پوشاک
- هدایا و گل
- خدمات مسافرتی
- اسباب بازی
- بلیط فروشی
- اطلاعات

بررسی شرکت Dell

امروزه شرکت های کوچک و بزرگ با حرکات سراسیمه و شتابان بسرعت بسمت استفاده از محیط جدید (اینترنت) برای ارائه کالا و یا خدمات می باشند. علت این همه تعجیل و بنوعی شیدائی در چیست؟ شرکت Dell یکی از موفقترین شرکت های موجود در زمینه تجارت الکترونیکی است. بدین منظور شایسته است در این بخش به بررسی وضعیت شرکت فوق در زمینه تجارت الکترونیکی پرداخته و از این رهگذر از تجارب موجود استفاده کرد.

Dell یکی از صدها شرکتی است که کامپیوترهای شخصی تولیدی خود را در اختیار مشتریان حقیقی و یا حقوقی قرار می دهد. فعالیت اقتصادی Dell با درج آگهی در پشت جلد مجلات کامپیوتری و فروش کامپیوتر از طریق تلفن، آغاز گردید. امروزه حضور شرکت Dell در عرصه تجارت الکترونیکی بسرعت متداول و عمومی شده است .شرکت فوق ، قادر به ارائه کالاهای بیشماری از طریق وب شده است. بر اساس آمارهای موجود ، فروش روزانه Dell ، چهارده میلیون دلار بوده و تقریبا" ۲۵ درصد فروش این شرکت از طریق وب انجام می گیرد. شرکت Dell قبل از استفاده ازتجارت الکترونیکی، اکثر سفارشات خود را از طریق تلفن اخذ و با استفاده از پست آنها را برای خریداران خود ، ارسال می کرد. با توجه به فروش ۲۵ درصدی شرکت فوق از طریق وب می توان به جایگاه و اهمیت موضوع تجارت الکترونیکی بیش از گذشته واقف گردید. در این راستا می توان به موارد زیر اشاره کرد:

- در صورتیکه شرکت Dell توانسته باشد، میزان فروش از طریق تلفن را ۲۵ درصد کاهش و ۲۵ درصد به میزان فروش خود از طریق وب بیفزاید ، دلیل روشن و قاطعی برای وجود مزایای تجارت الکترونیکی وجود ندارد؟ Dell صرفا" کامپیوتر عرضه می نماید. در صورتیکه مدیریت فروش از طریق وب هزینه های کمتری را به یک سازمان تحمیل نماید و یا افرادیکه از طریق وب کالای خود را خریداری می نمایند ، اقدام به خرید تجهیزات کمکی دیگری نمایند و یا اگر هزینه های عملیات فروش از طریق وب بمراتب کمترشده و یا اگر ارائه کالا بر روی وب باعث افزایش خریداران و حجم عملیات فروش گردد، استفاده از تجارت الکترونیکی برای شرکت Dell مقرون بصرفه و توام با افزایش بهره وری بوده است.
- در صورتیکه شرکت Dell ، در فرآیند فروش کالا از طریق وب ، فروش سنتی و مبتنی بر تلفن خود را از دست ندهد، چه اتفاقی می افتد؟این موضوع می تواند صحت داشته باشد ، این موضوع به تمایل عده ای برای خرید کالا از طریق وب

بستگی خواهد داشت . گرایش بسمت خرید از طریق اینترنت بصورت یک نیاز مطرح شده است و از این بابت نگرانی چندانی وجود نخواهد داشت.

- در رابطه با فروش عقیده ای وجود دارد که: زمانیکه یک مشتری کار خود را با یک فروشنده آغاز می نماید، نگهداری آن مشتری برای فروشنده بمراتب راحت تر از جذب مشتریان جدید است. بنابراین در صورتیکه تصمیم به ایجاد یک وب سایت زودتر اتحاذ گردد، نسبت به سایر فروشندگان که بعدا" تصمیم فوق را اتخاذ خواهند کرد، پیشقدم خواهید بود. شرکت Dell سایت خود را خیلی زود طراحی و پیاده سازی نموده و از این طریق از سایر رقبای خود پیشی گرفته است

عوامل سه گانه فوق، دلایل عمده بسمت استفاده از تجارت الکترونیکی است.

گیرائی تجارت الکترونیکی

دلایل زیر علل گیرائی و جاذبه فراوان تجارت الکترونیکی است:

- کاهش هزینه ها . در صورتیکه سایت تجارت الکترونیکی بخوبی پیاده سازی گردد ، هزینه های مربوط به ثبت سفارش قبل از ارائه کالا و هزینه های خدمات پس از فروش بعد از ارائه کالا کاهش می یابد.
- خرید بیشتر در هر تراکنش. سایت آمازون ویژگی را ارائه می دهد که در فروشگاههای معمولی نظیر آن وجود ندارد. زمانیکه مشخصات یک کتاب را مطالعه می نمائید، می توان بخشی با نام " افرادیکه کتاب فوق را سفارش داده اند ، چه چیزهای دیگری را خریداری نموده اند"، را نیز مشاهده نمود. بدین ترتیب امکان مشاهده سایر کتب مرتبط که سایرین خرید نموده اند، فراهم می گردد.بنابراین امکان خرید کتب بیشتر توسط مراجعه کنندگان به سایت نسبت به یک کتابفروشی معمولی بوجود خواهد آمد.
- در صورتیکه وب سایت بگونه ای طراحی شده باشد که با سایر مراحل مربوط به تجارت درگیر شده باشد، امکان اخذ اطلاعات بیشتری در رابطه با وضعیت کالای خریداری شده برای مشتریان وجود خواهد داشت. مثلا" در صورتیکه شرکت

Dell وضعیت هر کامپیوتر را از مرحله تولید تا عرضه ، ثبت نماید، مشتریان در هر لحظه قادر به مشاهده آخرین وضعیت سفارش خود خواهند بود.

- با استفاده از تجارت الکترونیکی افراد قادر به انتخاب کالای خود با روش های متفاوتی خواهند بود. وب سایت های موجود در این زمینه امکانات زیر را ارائه خواهند داد:
  - امکان ثبت یک سفارش طی چند روز
  - امکان پیکربندی محصول و مشاهده قیمت های واقعی
  - امکان ایجاد آسان سفارش های اختصاصی پیچیده
  - امکان مقایسه قیمت کالا بین چندین فروشنده
  - امکان جستجوی آسان برای کاتولوگ های مورد نیاز
- کاتولوگ های بزرگتر. یک شرکت قادر به ایجاد یک کاتولوگ بر روی وب بوده که هرگز امکان ارسال آن از طریق پست وجود نخواهد داشت. مثلا" آمازون بیش از سه میلیون کتاب را بفروش می رساند، اطلاعات مربوط به کتب فوق از طریق سایت آمازون ارائه ودر اختیار مراجعه کنندگان قرار می گیرد، ارسال اطلاعات فوق از طریق پست، بسیار مشکل و یا غیرممکن بنظر می آید.
- بهبود ارتباط متقابل با مشتریان. با طراحی مناسب سایت و استفاده از ابزار های مربوطه، امکان برقراری ارتباط متقابل با مشتریان با روش های مطمئن تر و بدون صرف هزینه، فراهم می گردد. مثلا" مشتری پس از ثبت سفارش با دریافت یک نامه الکترونیکی از ثبت سفارش خود مطمئن شده و یا در صورت ارسال کالا برای مشتری، می توان از طریق نامه الکترونیکی وی را مطلع نمود. همواره یک مشتری راضی و خوشحال تمایل به خرید مجدد از شرکت و یا موسسه ارائه دهنده کالا را خواهد داشت.

در رابطه با تجارت الکترونیکی ذکر یک نکته دیگر ضروری بنظر می رسد. تجارت الکترونیکی به افراد و یا سازمانها و موسسات امکان ایجاد مدل های کاملا" جدید تجاری

را خواهد داد. در شرکت های تجاری مبتنی بر ثبت سفارش پستی، هزینه های زیادی صرف چاپ و ارسال کاتولوگ ها، پاسخگوئی به تلفن ها و ردیابی سفارشات، میگردد. در تجارت الکترونیکی، هزینه توزیع کاتولوگ و ردیابی سفارشات بسمت صفر میل خواهد کرد. بدین ترتیب امکان عرضه کالا با قیمت ارزانتر فرام خواهد شد.

جنبه های ساده و سخت تجارت الکترونیکی

مواردیکه از آنها بعنوان عملیات دشوار و سخت در رابطه با تجارت الکترونیکی یاد می شود ، عبارتند از:

- ترافیک موجود بر روی سایت
- ترافیک مراجعات ثانویه بر روی سایت
- تمایز خود با سایر رقباء
- تمایل افراد به خرید کالا از سایت .مراجعه به سایت یک موضوع و خرید از سایت موضوعی دیگر است.
- ارتباط و تعامل سایت تجارت الکترونیکی با سایر داده های موجود در سازمان

امروزه بر روی اینترنت سایت های بیشماری وجود داشته و ایجاد یک سایت جدید تجارت الکترونیکی کار مشکلی نیست ولی جذب مخاطبین جهت مراجعه به سایت و خرید از آن ، مهمترین مسئله موجود در این زمینه است.

مواردیکه از آنها بعنوان عملیات ساده در رابطه با تجارت الکترونیکی یاد می شود،

عبارتند از :

- ایجاد یک وب سایت
- اخذ سفارشات
- پذیرش پرداخت

ایجاد یک سایت تجارت الکترونیکی

در زمان ایجاد یک سایت تجارت الکترونیکی موارد زیر می بایست مورد توجه قرار گیرد:

- تامین کنندگان . بدون وجود تامین کنندگان خوب امکان عرضه کالا وجود نخواهد داشت.
- قیمت . یکی از مهمترین بخش های تجارت الکترونیکی ، عرضه کالا با قیمت مناسب است . امکان مقایسه قیمت یک کالا بسادگی برای مشتریان وجود داشته و همواره قیمت یک کالا با موارد مشابه که از طریق سایر فروشندگان ارائه می گردد ، مقایسه خواهد شد.
- ارتباطات با مشتری . تجارت الکترونیکی مجموعه ای متنوع از روش های موجود جهت برقراری ارتباط با مشتری را ارائه می نماید. پست الکترونیکی ، پایگاه های دانش ، تالارهای مباحثه ، اتاق های گفتگو و ... نمونه هائی در این زمینه می باشند. مشتری همواره می بایست احساس نماید که در صورت بروز مشکل و یا درخواست اطلاعات بیشتر ، بدون پاسخ نخواهند ماند.
- توزیع کالا ، خدمات پس از فروش و امکان برگشت از فروش از جمله مواردی است که در موفقیت یک سایت تجارت الکترونیک نقش بسزائی دارد.

در زمان ایجاد یک سایت تجارت الکترونیکی ، قابلیت های زیر نیز می تواند عرضه و باعث موفقیت در امر تجارت الکترونیکی گردد:

- ارسال هدیه (جایزه)
- استفاده از برنامه های همبستگی
- تخفیف های ویژه
- برنامه های خریدار تکراری
- فروش ادواری و فصلی

نرم افزار مربوط به تجارت الکترونیکی می بایست امکانات فوق را فراهم نماید، درغیراینصورت انجام هر یک از موارد فوق با مشکل مواجه می گردد.

برنامه های همبستگی

یکی از بخش های مهم در زمینه تجارت الکترونیکی توجه و استفاده از برنامه های همبستگی (انجمنی) می باشد. ویژگی فوق توسط آمازون بخدمت گرفته شده است. آمازون این امکان را ارائه نموده تا هر شخص قادر به پیکربندی یک فروشگاه کتاب اختصاصی باشد. زمانیکه از هر یک از کتابفروشی های فوق ، کتابی خریداری می گردد، فردی که دارای کتابفروشی مربوطه است ، کمیسیونی (حداکثر ۱۵ درصد قیمت کتاب) را از آمازون دریافت می نماید. برنامه همبستگی، قابلیت های زیادی را در اختیار آمازون قرار می دهد . مدل فوق امروزه توسط هزاران سایت تجارت الکترونیکی دیگر مورد توجه قرار گرفته و از آن استفاده می گردد.

یکی از گرایشات جدید در زمینه برنامه های همبستگی، روش CPC link (Cost Per click) است. در این راستا بر روی سایت، یک لینک مربوط به سایت دیگر قرار گرفته و زمانیکه بر روی لینک فوق کلیک گردد، توسط شرکت مربوطه به شما مبلغی پرداخت می گردد. روش فوق، مدلی میانه بین روش های تبلیغاتی مبتنی بر Banner و برنامه های همبستگی مبتنی بر کمیسیون است . در روش تبلیغاتی مبتنی بر Banner، شرکت تبلیغ کننده تمام ریسک را بر عهده می گیرد. در صورتیکه فردی بر روی Banner کلیک ننماید، تبلیغ کننده پول خود را از دست داده است. در روش اخذ کمیسیون، تمام ریسک بر عهده وب سایت است. در صورتیکه وب سایت تعداد زیادی مشتری را به سایت تجارت الکترونیکی ارسال (هدایت) ولی هیچکدام از آنها کالائی را خریداری ننمایند ، مبلغی به وب سایت پرداخت نخواهد شد. در روش CPC دو طرف ریسک موجود را بصورت مشترک قبول می نمایند.

پیاده سازی یک سایت تجارت الکترونیک

سه روش عمده برای پیاده سازی یک سایت تجارت الکترونیک وجود دارد:

- **Enterprise Computing** . در روش فوق شرکت و یا موسسه مربوط اقدام به تهیه سخت افزار ، نرم افزار و کارشناسان ورزیده به منظور ایجاد وب سایت تجارت الکترونیکی خود می نماید. آمازون و سایر شرکت های بزرگ از روش فوق استفاده می نمایند. انتخاب روش فوق مشروط به وجود عوامل زیر است

  – شرکت مربوطه دارای ترافیک بسیار بالائی است (چندین میلیون در هر ماه)

  – شرکت مربوطه دارای یک بانک اطلاعاتی بزرگ بوده که شامل کاتولوگ های مربوط به محصولات است (مخصوصا" اگر کاتولوگ ها بسرعت تغییرمی یابند).

  – شرکت مربوطه دارای یک چرخه فروش پیچیده بوده که مستلزم استفاده از فرم های اختصاصی ، جداول متفاوت قیمت و ... است .

  – شرکت مربوطه دارای سایر پردازش های تجاری بوده و قصد ارتباط وپیوستگی آنها با سایت تجارت الکترونیکی وجود دارد.

- **سرویس های میزبانی مجازی** . فروشنده تجهیزات و نرم افزارهای مربوط را بعنوان یک بسته نرم افزاری اختصاصی عرضه می نماید. بخشی از بسته نرم افزاری شامل امنیت است . دستیابی به بانک اطلاعاتی نیز بخش دیگری از بسته نرم افزاری خواهد بود. با استفاده از پتانسیل های موجود در ادامه شرکت مربوطه می تواند با بخدمت گرفتن طراحان وب و پیاده کنندگان مربوطه اقدام به ایجاد و نگهداری سایت تجارت الکترونیکی خود نماید.

- **تجارت الکترونیکی ساده** . اکثر سازمانها و شرکت ها از روش فوق برای پیاده سازی سایت تجارت الکترونیکی استفاده می نمایند.سیستم شامل مجموعه ای از فرم های ساده بوده که توسط متقاضی تکمیل می گردند. نرم افزار مربوطه در ادامه تمام صفحات وب ذیربط را تولید می نماید.

یادگیری الکترونیکی

اینترنت در عرصه های آموزشی نیز چالش های جدیدی را ایجاد کرده است. استفاده از زیرساخت اینترنت برای آموزش، در سالیان اخیر مورد توجه کارشناسان و مراکز علمی قرار گرفته است. آموزش الکترونیکی، آموزش مبتنی بر کامپیوتر (CBT)، آموزش مبتنی بر اینترنت (IBT) و آموزش مبتنی بر وب (WBT) نمونه اسامی انتخاب شده برای روش های جدید آموزشی می باشند. آموزش (یاد دادن و یاد گیری)، طی سالیان آینده با انقلابی بزرگ روبرو خواهد شد. امکانات سخت افزاری و نرم افراری موجود، بشریت را به سمت یک انقلاب بزرگ آموزشی سوق می دهد. آموزش های Online از سال ۱۹۹۰ مطرح و همزمان با رشد تجهیزات و امکانات مربوطه در دهه گذشته، گام های موثری در این زمینه برداشته شده و اینک در نقطه عطفی قرار گرفته است. آشنائی با سیستم های آموزشی جدید برای تمامی دست اندرکاران امر آموزش، حائز اهمیت است. اگر دانائی را عین توانائی بدانیم ، جوامعی از بشریت به توانائی و خود باوری خواهند رسید که زیر ساخت مناسبی را برای سیستم های آموزشی خود انتخاب و بر همین اساس حرکات هدفمند و سیستماتیک آموزشی را با تاکید بر عناصر متفاوت موجود در یک سیستم آموزشی، آغاز نمایند. آموزش الکترونیکی فرصت مناسبی را برای تمامی دست اندرکاران سیستم های آموزشی فراهم نموده است تا بتوانند با بهره گیری از آخرین فن آوری های موجود، مهمترین رسالت خود را که همان آموزش است با سرعت وکیفیتی مطلوب دراختیار متقاضیان قرار دهند.

آموزش الکترونیکی چیست ؟

آموزش الکترونیکی، امکان فراگیری مستقل از زمان و مکان را برای دانش پژوهان فراهم می آورد. جایگاه کامپیوتر در آموزش های الکترونیکی بسیار حائز اهمیت است.

با پیکربندی مناسب کامپیوتر(سخت افزار، نرم افزار و شبکه)، امکان استفاده از آموزش های

الکترونیکی برای علاقه مندان فراهم می گردد. عملکرد کامپیوتر در آموزش های الکترونیکی نظیر عملکرد موبایل در ارتباطات است. با استفاده و پیکربندی مناسب موبایل امکان برقراری ارتباط مستقل از زمان و مکان خاص برای افراد بوجود می آید. آموزش الکترونیکی می تواند مبتنی بر CD-ROM ، شبکه، اینترانت و یا اینترنت باشد. آموزش الکترونیکی برای ارائه محتوی از عناصر اطلاعاتی با فرمت های متفاوت نظیر: متن ، ویدئو ، صدا، انیمیشن، گرافیک و محیط های مجازی و یا شبیه سازی شده استفاده می نماید. تجارب بدست آمده از آموزش های الکترونیکی بمراتب گسترده تر از تجارب آموزشی بدست آمده در یک کلاس درس سنتی است . آهنگ فراگیری در سیستم های آموزشی الکترونیکی از یک روند مشخص و سیستماتیک تبعیت کرده و مخاطبان خود را با هر نوع سلیقه و گرایش بسرعت جذب می نماید.

آموزش های الکترونیکی رمز موفقیت خود را در شیوه ارائه، نوع محتویات و توزیع (عرضه) مناسب می دانند. در آموزش های الکترونیکی از اغلب مسائل موجود در آموزش های سنتی نظیر : سخنرانی های یکطرفه، تعامل و ارتباط ضعیف با فراگیران، اجتناب می گردد. با استفاده از نرم افزارهای مربوط به سیستم های آموزش الکترونیکی می توان بسرعت محیط های آموزشی موثر و کارآ را با بهره گیری از عناصر متفاوت آموزشی ایجاد کرد.

سطوح آموزش الکترونیکی

آموزش الکترونیکی در چهار گروه عمده طبقه بندی می گردد. گروه های فوق سطوح متفاوت آموزشی از ابتدائی تا سطوح پیشرفته را تضمین می نمایند:

- **پایگاه های دانش** . پایگاه های دانش و اطلاعات خود بعنوان یک آموزش واقعی در نظر گرفته نمی شوند. بانک های اطلاعاتی شکل اولیه ای از آموزش الکترونیکی می باشند. بانک های اطلاعاتی فوق را می توان در سایت های نرم افزاری متعدد، در اینترنت مشاهده نمود. بانک های اطلاعاتی با یک روش سیستماتیک قادر به ارائه توضیحات و راهنمائی های ضروری در ارتباط با

سوالات مطرح شده در رابطه با نرم افزار می باشند. در این راستا دستورالعمل های لازم به منظور انجام عملیات خاص توسط یک نرم افزار بصورت مرحله به مرحله در اختیار متقاضیان قرار می گیرد.بانک های اطلاعاتی فوق ، اغلب بصورت متعامل با کاربران خود ارتباط برقرار می نمایند. مثلا" کاربران می توانند کلمات مورد نظر خود را در بخش مربوطه تایپ تا زمینه جستجو در بانک اطلاعاتی فراهم گردد. در این راستا امکان انتخاب موضوع مورد علاقه بر اساس لیست های مرتب شده (موضوعی و یا الفبائی) نیز وجود دارد.

- **حمایت فنی online** . حمایت online نیز نوع خاصی از آموزش الکترونیکی بوده که در مواردی شباهت هائی با پایگاه های دانش ، دارد. برای پیاده سازی حمایت های فنی online ، از روش های متعددی نظیر : تالارهای مباحثه، اتاق های گفتگو، سیستم های BBS ، پست الکترونیکی و یا ارسال پیام فوری و زنده ، استفاده می شود. سیستم های فوق تعامل بمراتب بیشتری را نسبت به پایگاه های دانش با مخاطب ، برقرار می نمایند.
- **آموزش نامتقارن** . سیستم فوق در آموزش های اولیه الکترونیکی استفاده می گردید. در روش فوق امکان خود آموزی با محوریت فراگیران فراهم می گردد. برای پیاده سازی و اجرای سیستم فوق از امکانات و روش های متعددی نظیر: آموزش های مبتنی بر CD-ROM ، اینترانت و یا اینترنت استفاده می گردد. دستیابی به مجموعه ای از دستورالعمل ها به منظور انجام یک عملیات خاص از طریق سیستم های BBS ، گروه ها و تالارهای متفاوت مباحثه و پست الکترونیکی نمونه هائی از امکانات ارائه شده توسط سیستم های فوق می باشند. در برخی موارد سیستم های فوق، بصورت کاملا" خود آموز بوده و از لینک های خاصی برای مراجعه به منابع متفاوت استفاده می گردد. دراین نوع سیستم ها، از مربیان آموزشی که بصورت زنده فعالیت های آموزشی فراگیران را مدیریت

می نمایند، استفاده نمی گردد. چارچوب و ساختار ارائه موضوع و محتوی اغلب بصورت خودآموز با هدایت لینک های تعریف شده در موضوعات متفاوت است.

- **آموزش همزمان** . آموزش همزمان بصورت بلادرنگ با کمک یک مربی آموزشی که بصورت زنده ناظر تمام فعالیت های آموزشی فراگیران است انجام می گیرد. در سیستم فوق، فراگیران با ورود به کلاس مجازی، قادر به برقراری ارتباط مستقیم با مربی و سایر فراگیران موجود در کلاس خواهند بود. در این نوع آموزش الکترونیکی، تمام ویژگی های یک کلاس درس بصورت مجازی شبیه سازی و در اختیار مربی و فراگیران قرار می گیرد. مثلا" می توان بصورت مجازی دست خود را برای سوال کردن بالا برده و یا حتی از یک تخته سیاه مجازی استفاده و محتویات نوشته شده بر روی آن را مشاهده نمود. جلسات آموزشی ممکن است صرفا" در حد و اندازه یک جلسه بوده و یا هفته ها، ماه ها و یا حتی سال ها، بطول انجامد. این نوع آموزش ها معمولا" از طریق وب سایت های اینترنت، کنفرانس های صوتی و یا تصویری ، اینترنت تلفنی انجام می گیرد.

روانشناسی یادگیری

چه نوع تحولات و یا اتفاقاتی در مغز انسان در زمان فراگیری، بوجود می آید؟ آموزش در ابتدا نیازمند محرک های لازم است .به منظور فراگیری موثر و کارآ ، محرک های موجود می بایست نگهداری گردند. متاسفانه سیستم های نرونی (عصبی) موجود در مغز که مسئول کنترل محرک ها و ذخیره سازی اطلاعات در حافظه می باشد، بسرعت دچار خستگی می گردند (پس از گذشت چند دقیقه). بدین ترتیب آنها نیازمند بازسازی در فواصل بین سه تا پنج دقیقه می باشند، در غیر اینصورت میزان پاسخگوئی و فراگیری آنها دچار افت می گردد. آنها بسرعت بازسازی می گردند، سیستم آموزشی می بایست بسرعت با خستگی و دلزدگی بوجود آمده برای فراگیران برخورد مناسب را داشته ، تا امکان یادگیری موثرتر بوجود آید.

یادگیری بر اساس الگو ها، موثرترین مدل یادگیری محسوب می گردد. در این روش، الگوها از مجموعه ای به مجموعه دیگر جابجا می گردند. الگوهائی که نرون های مربوط بخود را مسئول پاسخگوئی خواهند کرد، از اطلاعات متفاوت در محل های متفاوت مغز استفاده می نمایند . مثلا"

- **گوش دادن به یک حقیقت** . زمانیک آرد با تخم مرغ ترکیب می گردد، خمیری بوجود می آید که می توان آن را به قطعاتی به منظور ایجاد ماکارونی برش داد.
- **ارتباط یک مفهوم با یک حقیقت** . غذا که دارای کربوهیدرات بالائی است، برای تولید انرژی بدن لازم است.
- **تجسم دو چیز بایکدیگر** . تیم های ورزشی به انرژی سریع نیاز داشته و آن را از طریق کربوهیدرات تامین می نمایند، بنابراینن قبل از بازی یک وعده غذا مناسب خواهند داشت.

سیستم های فوق با یکدیگر مرتبط بوده و از طریق همکاری بایکدیگر حافظه را شکل خواهند داد (یادگیری) هدف شکل دهی حافظه، در هریک از سیستم های نرونی مربوطه است. بنابراین اطلاعاتی که بگونه ای طراحی می گردند تا از یک سیستم نرونی به سیستم نرونی دیگر حرکت نمایند، دارای کارآئی بیشتری در رابطه با یادگیری می باشند.

یادگیری الکترونیکی به چه صورت نگهداشت اطلاعات را بهبود می بخشد ؟

آموزش علاوه بر استفاده از سیستم های نرونی مورد نیاز ، مستلزم استفاده از عناصر دیگر نظیر : ارتباط متقابل، تخیل و فیدبک است. یادگیری الکترونیکی با استفاده از عناصر متفاوت، که باعث ایجاد عناصر جدید آموزشی می گردد ، فرآیند فراگیری را جذاب تر خواهد کرد. ایجاد جذابیت در یادگیری یکی از دلایل موفقیت آموزش های الکترونیکی است . در صورتیکه از عناصر جدید در سیستم های آموزش الکترونیکی استفاده نگردد، عملا" جذابیت های لازم برای آموزش را از دست داده ایم. برای موفقیت در آموزش های الکترونیکی نکات زیر می بایست مورد توجه قرار گیرد.

- بررسی نوع محتویات . استفاده از تصاویر، صدا و متن و ترکیب مناسب آنها با یکدیگر پیامدهای مثبتی را بدنبال خواهد داشت.
- ارتباط متقابل با فراگیران بگونه ای که ایجاد محرک های لازم را تضمین نماید. استفاده از بازیها ، امتحانات کوتاه مدت برای اخذ فیدبک سریع از فراگیران مناسب ترین روش برای سنجش میزان موفقیت در آموزش است.
- ایجاد فیدبک های سریع . دوره های آموزش الکترونیکی می بایست از روش هائی به منظور اخذ فید بک سریع استفاده تا در صورت اشکال و یا عدم موفقیت، سریعا" نسبت به برطرف نمودن آن اقدام نمایند. فیدبک های مربوطه می بایست در سریعترین زمان ممکن اخذ گردند. آموزش در هر مرحله بر اساس آموزش در مرحله قبل ایجاد می گردد. بنابراین تشخیص و اخذ فیدبک های سریع، مراحل متفاوت آموزشی را بدرستی تبین خواهد کرد. در صورتیکه در یک مرحله موفقیتی حاصل نشده باشد، مرحله بعد که بر اساس مرحله قبل ایجاد شده است، در امر آموزش توفیق چندانی ایجاد نخواهد کرد.
- ارتباطات صمیمی با سایر فراگیران و مربیان الکترونیکی. استفاده از اتاق های گفتگو، تالارهای مباحثه، پیام های فوری و پست الکترونیکی در ایجاد ارتباط متقابل با فراگیران الکترونیکی بسیار موثر و کارساز خواهد بود. ایجاد کمیته های Online بطرز چشمگیری در عملکرد برنامه های آموزشی تاثیر خواهد داشت.

آموزش های الکترونیکی به فراگیران این امکان را خواهد داد تا هر فرد با توجه به مسایل و توانائی خود، آهنگ یادگیری را خود مشخص نماید. در چنین مواردی، فراگیران در صورتیکه به دلایلی، چند روزی از سیستم استفاده ننمایند و از آموزش دور باشند، پس از برطرف شدن مشکلات، مجددا" قادر به ادامه آموزش خواهند بود. دوره های آموزشی مبتنی بر آموزش الکترونیکی دارای عناصر قابل کنترلی بوده که توسط کاربران استفاده می گردند. عناصر کنترلی فوق در کلاس ها ی آموزش معمولی استفاده نشده و با استفاده از آنان در آموزش های الکترونیکی، فراگیران قادر به کنترل فرآیند آموزش،

خواهند بود. قابلیت تنظیم آهنگ آموزش توسط فراگیران یکی از دلایل مهم در رابطه با موثر بودن آموزش های الکترونیکی است.

پست الکترونیکی

شهروندان اینترنت روزانه میلیون ها نامه الکترونیکی را برای یکدیگر ارسال می نمایند. مبادله نامه های الکترونیکی یکی از اولین سرویس های اینترنت محسوب شده و امروزه از آن به عنوان یک ابزار ارتباطی قدرتمند استفاده می گردد. در زمان ارسال یک نامه الکترونیکی ، فرآیند گسترده و مسیری طولانی طی خواهد شد.

یک پیام E-Mail

اولین پیام ارسال شده توسط نامه الکترونیکی در سال ۱۹۷۱ توسط مهندسی با نام " Ray Tomlinson" انجام شده است . قبل از تحقق رویداد فوق ، صرفا" امکان ارسال پیام برای کاربران موجود بر روی یک کامپیوتر میسر بود. پیام ارسالی توسط Tomlinson قابلیت ارسال پیام به سایر ماشین های موجود بر روی اینترنت با استفاده از علامت "@" به منظور مشخص نمودن ماشین دریافت کننده بود. E-Mail ، یک پیام متنی ساده است که برای گیرنده پیام ارسال می گردد. نامه های الکترونیکی در ابتدا و هم اینک اغلب بصورت متن های کوتاه می باشند. در برخی موارد ممکن است، فرستندگان نامه های الکترونیکی با افزودن "ضمائم "، حجم یک نامه الکترونیکی را افزایش دهند.

سرویس گیرندگان E-mail

به منظور مشاهده نامه های الکترونیکی دریافت شده، می بایست از برنامه های سرویس گیرنده نامه های الکترونیکی استفاده کرد. برخی از کاربران از برنامه معروف outlook و یا outlook express شرکت مایکروسافت، Eudora و یا Pegasus بمنظور مشاهده نامه های الکترونیکی استفاده می نمایند. افرادیکه از خدمات پست الکترونیکی رایگان نظیر Hotmail و یا Yahoo استفاده می نمایند، از یک برنامه سرویس گیرنده که بصورت یک صفحه وب نمایش داده می شود ، استفاده

می نمایند. برنامه های سرویس گیرنده صرفنظر از نوع خود ، دارای وظایف زیر می باشند:

- نمایش لیست تمام پیام های موجود در صندوق پستی از طریق " عناوین پیام ها " . عنوان یک پیام مشخص کننده فرستنده، موضوع، تاریخ و زمان و اندازه پیام است.
- امکان انتخاب یک پیام از طریق عنوان آن فراهم شده ومطالعه محتویات پیام
- امکان ایجاد پیام های جدید و ارسال آنها وجود خواهد داشت . برای ارسال یک پیام می بایست آدرس گیرنده، موضوع پیام را مشخص و در ادامه محتویات پیام را تایپ کرد.
- اکثر برنامه های سرویس گیرنده پیام های الکترونیکی امکان اضافه کردن ضمائم به یک پیام را نیز فراهم می آورند. برنامه های فوق همچنین امکان ذخیره کردن ضمائم موجود در پیام های دریافت شده را نیز دارا می باشند.

یک سرویس دهنده ساده پست الکترونیکی

به منظور ارسال یک نامه الکترونیکی ، برنامه سرویس گیرنده موجود می بایست به یک سرویس دهنده پست الکترونیکی مرتبط گردد. برخی از ماشین های موجود بر روی اینترنت با نصب نرم افزارهای لازم بعنوان " سرویس دهنده " در شبکه ایفای وظیفه می نمایند. سرویس دهنده وب ، سرویس دهنده telnet ، سرویس دهنده Ftp و سرویس دهنده پست الکترونیکی ، نمونه هائی از سرویس دهندگان موجود در اینترنت می باشند. میلیون ها سرویس دهنده بر روی اینترنت به ارائه خدمات و سرویس های مورد نظر به سرویس گیرندگان فعالیت می نمایند. برنامه های نصب شده بر روی سرویس دهندگان بصورت شبانه روزی در حالت اجراء بوده و به پورت های خاصی گوش فرا می دهند. این نوع برنامه ها در انتظار ارتباط سایر برنامه ها (سرویس گیرندگان) از طریق پورت مربوطه می باشند. یک برنامه سرویس دهنده پست الکترونیکی در ساده ترین (حالت آموزشی) حالت بصورت زیر عمل می نماید:

- هر شخص بر روی سرویس دهنده دارای یک Account به منظور ارسال و دریافت نامه الکترونیکی است.
- برای هر یک از افرادیکه دارای Account می باشند، یک فایل ساده متنی در فولدر مورد نظر ذخیره می گردد.
- افرادیکه تمایل به ارسال نامه الکترونیکی برای شخص بخصوصی را داشته باشند، می بایست یک پیام متنی را با استفاده از یک برنامه سرویس گیرنده ارسال نمایند. پس از آماده نمون پیام ، با فشردن دکمه "ارسال"، پیام مورد نظر برای گیرنده ارسال خواهد شد. در این حالت برنامه سرویس گیرنده با برنامه سرویس دهنده ارتباط برقرار و پیام حاوی آدرس فرستنده، گیرنده و محتویات مورد نظر را برای سرویس دهنده مورد نظر ارسال می نماید.
- سرویس دهنده ممکن است اطلاعات دریافت شده را با یک فرمت مناسب به انتهای فایل متنی که برای هر فرد با نام Account وی ایجاد شده، اضافه می نماید.
- سرویس دهنده ممکن است اطلاعات دیگر نظیر : زمان و تاریخ دریافت پیام را نیز ذخیره نماید. در صورت ارسال نامه های الکترونیکی دیگر برای یک گیرنده خاص ، سرویس دهنده پیام های دریافت شده را به انتهای فایل متنی (حاوی پیام های مربوطه) اضافه می نماید. گیرنده پیام های الکترونیکی از برنامه سرویس گیرنده خود به منظور دریافت و مشاهده نامه های الکترونیکی استفاده می نماید:"
- برنامه سرویس گیرنده از سرویس دهنده می خواهد که یک نسخه از فایل متنی مربوط به شخص گیرنده را ارسال نماید.
- برنامه سرویس گیرنده از سرویس دهنده می خواهد که محتویات فایل متنی را حذف نماید.
- برنامه سرویس گیرنده قادر به ذخیره سازی فایل متنی حاوی پیام ها بر روی کامپیوتر خود است.

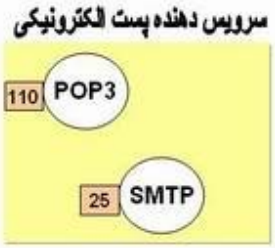
- در فایل متنی ذخیره شده بدنبال خطوطی باشد که با عنوان "از" وجود دارند.
- برنامه سرویس گیرنده قادر به نمایش لیست تمام پیام ها بر اساس عناوین مربوطه است.

مثال فوق صرفا" یک سیستم بسیار ساده ارسال و دریافت پست الکترونیکی را نشان می داد. در ادامه به بررسی یک سیستم واقعی پست الکترونیکی خواهیم پرداخت.

سیستم پست الکترونیکی واقعی

سیستم واقعی پست الکترونیکی دارای دو سرویس دهنده متفاوت بوده که بر روی یک ماشین اجراء می گردند.

یکی از سرویس دهندگان، سرویس دهنده **SMTP** (Simple Mail Transfer Protocol) بوده و مستولیت پیام های ارسالی (خروج) نامه های الکترونیکی، را برعهده دارد. سرویس دهنده دوم، **POP3** (Post office Protocol) نامیده شده و مسدولیت پیام های دریافتی (ورود) را برعهده دارد. شکل زیر جایگاه هر یک از سرویس دهندگان اشاره شده را نشان می دهد.



سرویس دهنده SMTP به پورت ۲۵ و سرویس دهنده POP3 به پورت ۱۱۰ گوش خواهند داد.

سرویس دهنده SMTP

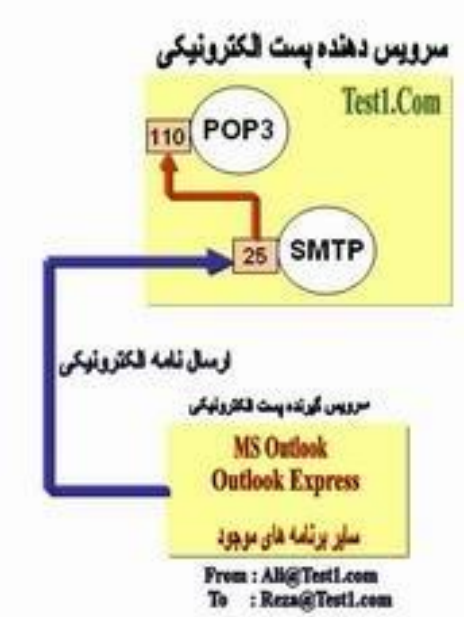
زمانیکه از طریق سرویس گیرنده خود اقدام به ارسال نامه الکترونیکی می نمائید، برنامه سرویس گیرنده با سرویس دهنده SMTP به منظور ارسال نامه های الکترونیکی، ارتباط برقرار می نماید. سرویس دهنده SMTP موجود، ممکن است با سایر سرویس دهندگان

SMTP به منظور ارسال (توزیع) نامه الکترونیکی ارتباط برقرار نماید. شکل زیر نحوه عملکرد سرویس دهنده فوق را نشان می دهد.

کاربران به منظور ارسال نامه الکترونیکی توسط برنامه سرویس گیرنده، می بایست تنظیمات لازم را انجام دهند. فرض کنید آدرس پست الکترونیکی شما Ali@Test1.com باشد، در زمان تنظیم پارامترهای برنامه سرویس گیرنده (بعنوان مثال: Outlook)، نام سرویس دهنده پست الکترونیکی می بایست مشخص گردد (فرض کنید نام سرویس دهنده پست الکترونیکی mail.test.com باشد). پس از آماده نمودن نامه الکترونیکی و فشردن دکمه "ارسال"، عملیات زیر انجام خواهد شد:

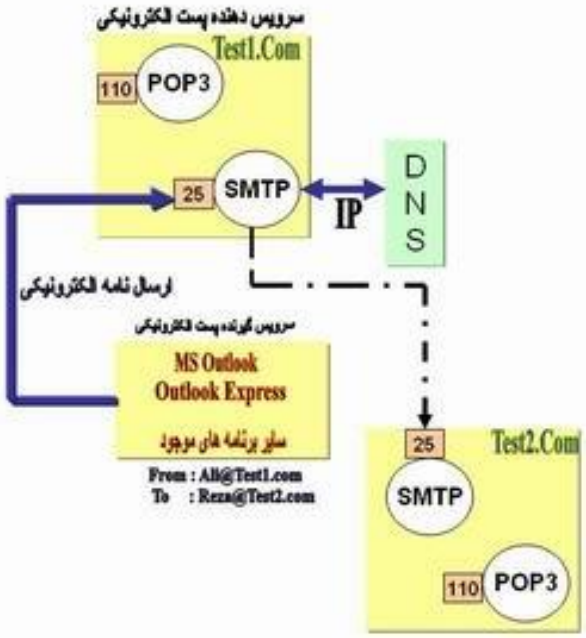
- برنامه Outlook express، با سرویس دهنده SMTP موجود در mail.test.com۱ از طریق پورت ۲۵ ، ارتباط برقرار می نماید.
- برنامه Outlook Express با سرویس دهنده SMTP مکالمه ای را برقرارو به سرویس دهنده SMTP ، آدرس های فرستنده و گیرنده و محتویات پیام را اعلان می نماید.
- سرویس دهنده SMTP آدرس گیرنده (بعنوان مثال Reza@test1.com) را به دو بخش مجزا تقسیم می نماید:
  - نام دریافت کننده (Reza)
  - نام حوزه (test1.com)

- در صورتیکه گیرنده پیام دارای صندوق پستی بر روی همان سرویس دهنده باشد ، سرویس دهنده SMTP پیام دریافت شده را بسادگی در اختیار سرویس دهنده POP3 قرار خواهد داد. در این زمینه از برنامه ای با نام " Delivery agent" (آژانس توزیع) استفاده می گردد. در صورتیکه گیرنده پیام بر روی حوزه ای دیگر باشد ، سرویس دهنده SMTP نیازمند برقراری ارتباط با حوزه مربوطه است .



- سرویس دهنده SMTP ، با DNS مربوط ارتباط و از او می خواهد که آدرس aIP مربوط به سرویس دهنده SMTP حوزه مربوطه را به اطلاع وی برساند. (فرض این است که گیرنده پیام دارای صندوق پستی بر روی همان کامپیوتر فرستده نیست). در ادامه DNS ، آدرس (و یا آدرس های) IP مربوط به سرویس دهنده (سرویس دهندگان) SMTP مربوط به حوزه مربوطه را اعلام می نماید.
- سرویس دهنده موجود در حوزه Test1.com با سرویس دهنده موجود در حوزه Test2.com از طریق پورت ۲۵ ، ارتباط برقرار می نماید. سرویس

دهنده SMTP موجود در حوزه Test2.com ، پیام ارسالی را دریافت و آن را در صندوق پستی مربوط به گیرنده قرار خواهد داد.



در صورتیکه سرویس دهنده موجود در حوزه Test1.com قادر به برقراری ارتباط با سرویس دهنده SMTP موجود در حوزه Test2.com نگردد ، پیام مورد نظر در محلی خاص در نوبت قرار می گیرد. سریس دهنده SMTP در اکثر ماشین ها از برنامه ای با نام Sendmail برای ارسال واقعی یک پیام الکترونیکی استفاده نموده و برای پیام های موجود در صف، از صفی با نام sendmail queue استفاده می گردد. برنامه Sendmail بصورت ادواری(تکراری) سعی در ارسال مجدد پیام های موجود در صف می نماید . مثلا" ممکن است هر ۱۵ دقیقه یکبار تلاش مجدد خود برای ارسال را انجام دهد. پس از گذشت چهار ساعت برای ارسال کننده نامه الکترونیکی ، پیامی مبنی بر وجود اشکال در ارسال نامه ، فرستاده می شود. پس از پنج روز، اکثر برنامه های پیکربندی Sendmail پیامی مبنی بر عدم موفقیت در توزیع پیام را برای ارسال می دارند.

مبادله اطلاعاتی بین سرویس گیرنده پست الکترونیکی و سرویس دهنده SMTP با استفاده از یک زبان ساده متنی و خوانا، با یکدیگر ارتباط برقرار می نمایند. در ابتدا برنامه سرویس گیرنده خود را معرفی ، آدرس فرستنده و گیرنده و محتویات پیام را مشخص خواهد کرد. (با استفاده از برنامه telnet می توان با سرویس دهنده پست الکترونیکی و از طریق پورت ۲۵ ارتباط برقرار کرد).سرویس دهنده SMTP از دستورات ساده ای نظیر HELLO,MAIL,RCPT,DATA و ... استفاده می نماید.

- HELLO. معرفی برنامه سرویس گیرنده
- EHLO . معرفی سرویس گیرنده و درخواست حالت توسه یافته
- MAIL FROM. مشخص کردن فرستنده
- RCPT TO . مشخص کردن گیرنده
- DATA . محتویات پیام را مشخص می کند.
- RESET . برای Reset نمودن استفاده می شود.
- QUIT . ارتباط را قطع می نماید.
- HELP . در رابطه با دستورات توضیحات لازم را ارائه می نماید.

سرویس دهنده POP3

زمانیکه با استفاده از برنامه سرویس گیرنده ، صندوق پستی خود را به منظور دریافت نامه های الکترونیکی بررسی می نمائید، برنامه فوق با سرویس دهنده POP3 از طریق پورت ۱۱۰ ارتباط برقرار می نماید. سرویس دهنده POP3 به یک نام Account و رمز عبور نیاز دارد. پس از تایید اعتبار و مجوز شما ، سرویس دهنده POP3 فایل های مربوطه را فعال و امکان دستیابی به آنان را فراهم می نماید.

رادیو اینترنتی

اینترنت در عرصه پخش صوت (صدا) و تصویر، نیز تحولات چشمگیری را بوجود آورده است. استفاده از رادیوهای اینترنتی، مهمترین تحول در زمینه استفاده از رادیو از سال ۱۹۲۰ است. رادیوهای اینترنتی از اواخر سال ۱۹۹۰ مورد توجه جدی قرار گرفته اند. با استفاده از رادیوهـای اینترنتی می توان از هر محل و توسط صرفا" یـک دستگاه کامپیوتر به اطلاعات منتشر شده، دستیابی پیدا کرد.

استفاده از رادیو به منظور نشر اطلاعات، از اوایل سال ۱۹۲۰ مطرح گردید. در سال ۱۹۵٤ همزمان با ابداع ترانزیستور، استفاده از رادیو بشدت رشد و متداول گردید. رادیوهای اینترنتی در اواخر قرن بیستم و اوایل قرن بیست و یکم مطرح و با توجه به زیرساخت اینترنت بسرعت با استقبال مواجه گردیدند. برای دستیابی به رادیوهای اینترنتی به یکدستگاه کامپیوتر شخصی و اینترنت نیاز است. دستیابی به اینترنت بصورت بدون کابل، امکان استفاده از رادیوهای اینترنتی را در اتومبیل، PDA و تلفن های سلولی فراهم کرده است. نسل جدید دستگاههای بدون کابل، دارای قابلیت های گسترده ای به منظور دستیابی به رادیوهای اینترنتی خواهند بود.

مزایای رادیوهای اینترنتی

ایستگاههای رادیوئی سنتی، دارای دو محدودیت عمده در رابطه با نشر اطلاعات می باشند:

- قدرت ایستگاه فرستنده (معمولا" یکصد miles)
- امواج رادیوئی قابل دسترس (صدها ایستگاه محلی ممکن است وجود داشته باشد

رادیوهای اینترنتی دارای محدودیت جغرافیائی نمی باشند. بنابراین انتشار اطلاعات توسط یک رادیوی اینترنتی در شرق، قابل شنیدن در غرب خواهد بود.

پتانسیل رادیوهای اینترنتی بسیار گسترده است. رادیوهای اینترنتی در مقایسه با رادیوهای سنتی که صرفا" از صوت برای پخش اطلاعات استفاده می نمایند، امکان استفاده از تصاویر، گرافیک، متن، لینک های مربوطه و ارتباط متقابل با شنونده را نیز ارائه می دهند.

با توجه به ماهیت عملکرد رادیوهای اینترنتی استفاده از آنان در موارد متعددی توصیه می گردد. مثلا" در یک سیستم آموزشی و یا آموزش های مبتنی بر وب، استفاده از رادیوهای اینترنتی به منظور نشر اطلاعات بسیار حائز اهمیت است. رادیوهای اینترنتی از طیف گسترده ای از امواج برای نشر اطلاعات خصوصا" در رابطه با موزیک استفاده می نمایند.

ایجاد یک ایستگاه رادیو اینترنتی

به منظور ایجاد یک ایستگاه رادیوئی اینترنتی به امکانات زیر نیاز خواهد بود:

- CD player
- نرم افزار های مربوط به تکثیر یک Track موزیک از یک CD به هارد دیسک کامپیوتر
- نرم افزارهای ویرایش و ضبط صدا
- میکروفن
- Mixer های صوتی
- Compressor ،Equalizer
- کارت صدا
- کامپیوتر اختصاصی بهمراه نرم افزار های encoder
- سرویس دهنده Streaming media

برای نشر اطلاعات از طریق رادیوهای اینترنتی مراحل زیر دنبال می گردد:

- اطلاعات صوتی از طریق یک کارت صدا به کامپیوتر مورد نظر وارد می گردند.
- یستم فوق، اطلاعات صوتی دریافتی را به فرمت Streaming تبدیل می نماید. اطلاعا ت صوتی دریافتی، نمونه سازی و پس از قشرده سازی آماده ارسال بر روی اینترنت خواهند شد.
- اطلاعات صوتی فشرده شده، برای سرویس دهنده ارسال می گردند. سرویس دهنده می بایست دارای یک پهنای باند بالا با اینترنت باشد.
- سرویس دهنده اقدام به ارسال اطلاعات صوتی بر روی اینترنت کرده و کامپیوترهای شنونده که دارای نرم افزارهای Player و یا Plug-in می باشند، قادر به شنیدن خواهند بود. نرم افزارهای فوق، اطلاعا ت صوتی stream دریافت شده از سرویس دهنده را به صوتی که قابل شنیدن توسط شنونده باشند، تبدیل می نمایند.

از دو روش متفاوت برای عرضه صوت بر روی اینترنت استفاده می شود: Download و Streaming media . در روش download ، یک فایل صوتی بر روی کامپیوتر کاربر ذخیره می گردد. فرمت های فشرده نظیر mp3، متداولترین فرمت فایل های صوتی برای Download کردن می باشند. (ارسال هر نوع فایل صوتی توسط وب سایت ها و یا سایت های Ftp امکان پذیر است).

در روش Streaming ، فایل صوتی ذخیره نمی گردد بلکه صرفا" پخش خواهد شد. انتشار اطلاعات بکمک روش فوق بصورت پیوسته و با بهره گیری از سه نرم افزار انجام می گیرد : Encode و Server و Player . نرم افزار encoder اطلاعات صوتی را به فرمت streaming تبدیل می نماید.

سرویس دهنده ،اطلاعات تبدیل شده را قابل دسترس بر روس اینترنت نموده و نرم افزار player ، مسدول بازیابی اطلاعات است. در پخش مستقیم، نرم افزارهای encoder و Streamer بصورت همزمان فعالیت می نمایند. اطلاعات صوتی از طریق کارت صدا به سیستم مربوطه تغذیه و پس از Encode نمودن آنها توسط نرم

افزار مربوطه بر روی سرویس دهنده streaming قرار خواهند گرفت. باتوجه به حجم بالای عملیات محاسباتی، سرویس دهنده Streaming می بایست یک سرویس دهنده قدرتمند و اختصاصی باشد.

بخش چهارم: شبکه

شبکه های کامپیوتری

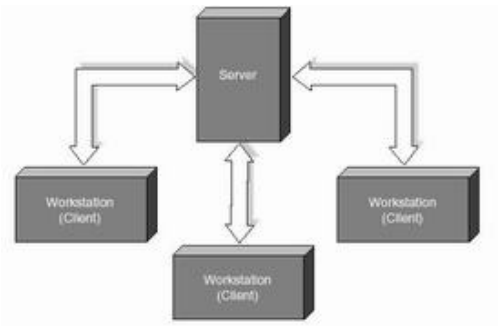
یک شبکه شامل مجموعه ای از دستگاهها (کامپیوتر، چاپگرو...) بوده که با استفاده از یک روش ارتباطی (کابل، امواج رادیوئی، ماهواره) و به منظور اشتراک منابع فیزیکی (چاپگر) و اشتراک منابع منطقی (فایل) به یکدیگر متصل می گردند. شبکه ها می توانند با یکدیگر نیز مرتبط شده و شامل زیر شبکه هائی باشند.

تقسیم بندی شبکه ها

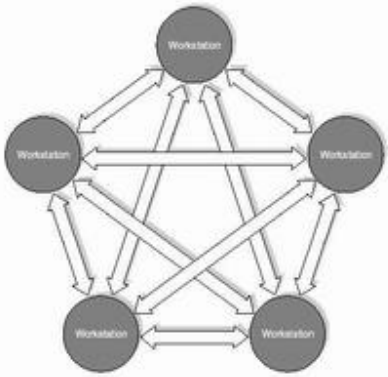
شبکه های کامپیوتری را بر اساس مولفه های متفاوتی تقسیم بندی می نمایند. در ادامه به برخی از متداولترین تقسیم بندی های موجود اشاره می گردد.

تقسیم بندی بر اساس نوع وظایف

کامپیوترهای موجود در شبکه را با توجه به نوع وظایف مربوطه به دوگروه عمده: سرویس دهندگان (Servers) و یا سرویس گیرندگان (Clients) تقسیم می نمایند. کامپیوترهائی در شبکه که برای سایرکامپیوترها سرویس ها وخدماتی را ارائه می نمایند، سرویس دهنده نامیده می گردند. کامپیوترهائی که از خدمات و سرویس های ارائه شده توسط سرویس دهندگان استفاده می کنند، سرویس گیرنده نامیده می شوند. در شبکه های Client-Server، یک کامپیوتر در شبکه نمی تواند هم به عنوان سرویس دهنده و هم به عنوان سرویس گیرنده، ایفای وظیفه نماید.



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



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

- **دو کامپیوتر شخصی** . یک شبکه می تواند شامل چند صد کامپیوتر باشد. حداقل یکی از کامپیوترها می بایست به عنوان سرویس دهنده مشخص گردد. (درصورتی که شبکه از نوع Client-Server باشد). سرویس دهنده، کامپیوتری است که هسته اساسی سیستم عامل بر روی آن نصب خواهد شد.
- **یک عدد کارت شبکه (NIC)** برای هر دستگاه. کارت شبکه نظیر کارت هائی است که برای مودم و صدا در کامپیوتر استفاده می گردد. کارت شبکه مسئول دریافت، انتقال، سازماندهی و ذخیره سازی موقت اطلاعات در طول شبکه است. به منظور انجام وظایف فوق کارت های شبکه دارای پردازنده، حافظه و گذرگاه اختصاصی خود هستند.

تقسیم بندی بر اساس توپولوژی

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

گماشت. عوامل مختلفی جهت انتخاب یک توپولوژی بهینه مطرح می شود. مهمترین این عوامل بشرح ذیل است:

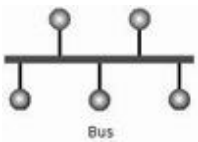
- **هزینه** . هر نوع محیط انتقال که برای شبکه LAN انتخاب گردد، در نهایت می بایست عملیات نصب شبکه در یک ساختمان پیاده سازی گردد. عملیات فوق فرآیندی طولانی جهت نصب کانال های مربوطه به کابل ها و محل عبور کابل ها در ساختمان است. در حالت ایده آل کابل کشی و ایجاد کانال های مربوطه می بایست قبل از تصرف و بکارگیری ساختمان انجام گرفته باشد. بهرحال می بایست هزینه نصب شبکه بهینه گردد.
- **انعطاف پذیری** . یکی از مزایای شبکه های LAN، توانائی پردازش داده ها و گستردگی و توزیع گره ها در یک محیط است. بدین ترتیب توان محاسباتی سیستم و منابع موجود در اختیار تمام استفاده کنندگان قرار خواهد گرفت. در ادارات همه چیز تغییر خواهد کرد.(لوازم اداری، اتاقها و ...). توپولوژی انتخابی می بایست بسادگی امکان تغییر پیکربندی در شبکه را فراهم نماید. مثلا" ایستگاهی را از نقطه ای به نقطه دیگر انتقال و یا قادر به ایجاد یک ایستگاه جدید در شبکه باشیم.

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

BUS
STAR
RING

توپولوژی BUS

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



مزایای توپولوژی BUS

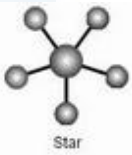
- **کم بودن طول کابل** . بدلیل استفاده از یک خط انتقال جهت اتصال تمام کامپیوترها، در توپولوژی فوق از کابل کمی استفاده می شود. موضوع فوق باعث پایین آمدن هزینه نصب و ایجاد تسهیلات لازم در جهت پشتیبانی شبکه خواهد بود.
- **ساختار ساده** . توپولوژی BUS دارای یک ساختار ساده است. در مدل فوق صرفا" از یک کابل برای انتقال اطلاعات استفاده می شود.
- **توسعه آسان**. یک کامپیوتر جدید را می توان براحتی در نقطه ای از شبکه اضافه کرد. در صورت اضافه شدن ایستگاههای بیشتر در یک سگمنت، می توان از تقویت کننده هائی به نام Repeater استفاده کرد.

معایب توپولوژی BUS

- **مشکل بودن عیب یابی** . با اینکه سادگی موجود در تویولوژی BUS امکان بروز اشتباه را کاهش می دهند، ولی در صورت بروز خطاء کشف آن ساده نخواهد بود. در شبکه هائی که از توپولوژی فوق استفاده می نمایند، کنترل شبکه در هر گره دارای مرکزیت نبوده و در صورت بروز خطاء می بایست نقاط زیادی به منظور تشخیص خطاء بازدید و بررسی گردند.
- **ایزوله کردن خطاء مشکل است**. در صورتی که یک کامپیوتر در توپولوژی فوق دچار مشکل گردد، می بایست کامپیوتر را در محلی که به شبکه متصل است رفع عیب نمود. در موارد خاص می توان یک گره را از شبکه جدا کرد. در حالتیکه اشکال در محیط انتقال باشد، تمام یک سگمنت می بایست از شبکه خارج گردد.
- **ماهیت تکرارکننده ها** . در مواردیکه برای توسعه شبکه از تکرارکننده ها استفاده می گردد، ممکن است در ساختار شبکه تغییراتی نیز داده شود. موضوع فوق مستلزم بکارگیری کابل بیشتر و اضافه نمودن اتصالات مخصوص شبکه است.

توپولوژی STAR

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



مزایای توپولوژی STAR

- **سادگی سرویس شبکه** . توپولوژی STAR شامل تعدادی از نقاط اتصالی در یک نقطه مرکزی است. ویژگی فوق تغییر در ساختار و سرویس شبکه را آسان می نماید.
- **در هر اتصال یکدستگاه** . نقاط اتصالی در شبکه ذاتا" مستعد اشکال هستند. در توپولوژی STAR اشکال در یک اتصال، باعث خروج آن خط از شبکه و سرویس و اشکال زدائی خط مزبور است. عملیات فوق تاثیری در عملکرد سایر کامپیوترهای موجود در شبکه نخواهد گذاشت.
- **کنترل مرکزی و عیب یابی** . با توجه به این مسئله که نقطه مرکزی مستقیما" به هر ایستگاه موجود در شبکه متصل است، اشکالات و ایرادات در شبکه بسادگی تشخیص و مهار خواهند گردید.
- **روش های ساده دستیابی** . هر اتصال در شبکه شامل یک نقطه مرکزی و یک گره جانبی است . در چنین حالتی دستیابی به محیط انتقال جهت ارسال و دریافت اطلاعات دارای الگوریتمی ساده خواهد بود.

معایب توپولوژی STAR

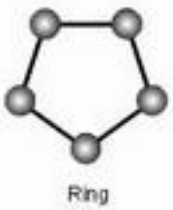
- **زیاد بودن طول کابل** . بدلیل اتصال مستقیم هر گره به نقطه مرکزی ، مقدار زیادی کابل مصرف می شود. با توجه به اینکه هزینه کابل نسبت به تمام شبکه،کم است،

تراکم در کانال کشی جهت کابل ها و مسائل مربوط به نصب و پشتیبانی آنها بطور قابل توجهی هزینه ها را افزایش خواهد داد.

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

توپولوژی RING

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



مزایای توپولوژی RING

- **کم بودن طول کابل** . طول کابلی که در این مدل بکار گرفته می شود، قابل مقایسه به توپولوژی BUS نبوده و طول کمی را در بردارد. ویژگی فوق باعث

کاهش تعداد اتصالات (کانکتور) در شبکه شده و ضریب اعتماد به شبکه را افزایش خواهد داد.

- **نیاز به فضائی خاص جهت انشعابات در کابل کشی نخواهد بود**.بدلیل استفاده از یک کابل جهت اتصال هر گره به گره همسایه اش، اختصاص محل هائی خاص به منظور کابل کشی ضرورتی نخواهد داشت.
- **مناسب جهت فیبر نوری** . استفاده از فیبر نوری باعث بالا رفتن نرخ سرعت انتقال اطلاعات در شبکه است. چون در توپولوژی فوق ترافیک داده ها در یک جهت است، می توان از فیبر نوری به منظور محیط انتقال استفاده کرد. در صورت تمایل می توان در هر بخش ازشبکه از یک نوع کابل به عنوان محیط انتقال استفاده کرد. مثلا" در محیط های ادرای از مدل های مسی و در محیط کارخانه از فیبر نوری استفاده کرد.

معایب توپولوژی RING

- **اشکال در یک گره باعث اشکال در تمام شبکه می گردد**. در صورت بروز اشکال در یک گره، تمام شبکه با اشکال مواجه خواهد شد. و تا زمانیکه گره معیوب از شبکه خارج نگردد، هیچگونه ترافیک اطلاعاتی را روی شبکه نمی توان داشت.
- **اشکال زدائی مشکل است** . بروز اشکال در یک گره می تواند روی تمام گرههای دیگر تاثیر گذار باشد. به منظور عیب یابی می بایست چندین گره بررسی تا گره مورد نظر پیدا گردد.
- **تغییر درساختارشبکه مشکل است** . در زمان گسترش و یا اصلاح حوزه جغرافیائی تحت پوشش شبکه، بدلیل ماهیت حلقوی شبکه مسائلی بوجود خواهد آمد.
- **توپولوژی بر روی نوع دستیابی تاثیر می گذارد**. هر گره در شبکه دارای مسئولیت عبور دادن داده ای است که از گره مجاور دریافت داشته است. قبل از

اینکه یک گره بتواند داده خود را ارسال نماید، می بایست به این اطمینان برسد که محیط انتقال برای استفاده قابل دستیابی است.

تقسیم بندی بر اساس حوزه جغرافی تحت پوشش .

شبکه های کامپیوتری با توجه به حوزه جغرافیائی تحت پوشش به سه گروه تقسیم می گردند:

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

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

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

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

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

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

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

کابل در شبکه

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

کابل Unshielded Twisted pair)UTP(

متداولترین نوع کابلی که در انتقال اطلاعات استفاده می گردد، کابل های بهم تابیده می باشند. این نوع کابل ها دارای دو رشته سیم به هم پیچیده بوده که هر دو نسبت زمین دارای یک امپدانس یکسان می باشند. بدین ترتیب امکان تاثیر پذیری این نوع کابل ها از کابل های مجاور و یا سایر منابع خارجی کاهش خواهد یافت. کابل های بهم تابیده دارای دو مدل متفاوت: Shielded (روکش دار) و Unshielded (بدون روکش) می باشند. کابل UTP نسبت به کابل STP بمراتب متداول تر بوده و در اکثر شبکه های محلی استفاده می گردد.

کیفیت کابل های UTP متغیر بوده و از کابل های معمولی استفاده شده برای تلفن تا کابل های با سرعت بالا را شامل می گردد. کابل دارای چهار زوج سیم بوده و درون یک روکش قرار می گیرند. هر زوج با تعداد مشخصی پیچ تابانده شده (در واحد اینچ) تا تاثیر پذیری آن از سایر زوج ها و یاسایر دستگاههای الکتریکی کاهش یابد.

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

Type	کاربرد
Cat 1	فقط صوت (کابل های تلفن)
Cat 2	داده با سرعت ٤ مگابیت در ثانیه
Cat 3	داده با سرعت ۱۰ مگابیت در ثانیه
Cat 4	داده با سرعت ۲۰ مگابیت در ثانیه
Cat 5	داده با سرعت ۱۰۰ مگابیت در ثانیه

مزایای کابل های بهم تابیده :

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

معایب کابل های بهم تابیده :

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

کانکتور استاندارد برای کابل هایUTP، از نوع RJ-45 می باشد. کانکتور فوق شباهت زیادی به کانکتورهای تلفن (RJ-11) دارد. هر یک از پین های کانکتور فوق می بایست بدرستی پیکربندی گردند. (RJ: Jack Registered)

کابل کواکسیال

یکی از مهمترین محیط های انتقال در مخابرات کابل کواکسیال و یا هم محور می باشد. این نوع کابل ها از سال ۱۹۳٦ برای انتقال اخبار و اطلاعات در دنیار به کار گرفته شده اند. در این نوع کابل ها، دو سیم تشکیل دهنده یک زوج، از حالت متقارن خارج شده و هر زوج از یک سیم در مغز و یک لایه مسی بافته شده در اطراف آن تشکیل می گردد. در نوع دیگر کابل های کواکسیال، به حای لایه مسی بافته شده، از تیوپ مسی استوانه ای استفاده می شود. ماده ای پلاستیکی این دو هادی را از یکدیگر جدا می کند. ماده پلاستیکی ممکن است بصورت دیسکهای پلاستیکی یا شیشه ای در فواصل مختلف استفاده و مانع از تماس دو هادی با یکدیگر شود و یا ممکن است دو هادی در تمام طول کابل بوسیله مواد پلاستیکی از یکدیگر جدا گردند.

مزایای کابل های کواکسیال :

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

معایب کابل های کواکسیال :

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

از کانکتورهای (**BNC**(Bayone -Neill - Concelman بهمراه کابل های کواکسیال استفاده می گردد. اغلب کارت های شبکه دارای کانکتورهای لازم در این خصوص می باشند.

شبکه و انواع آن

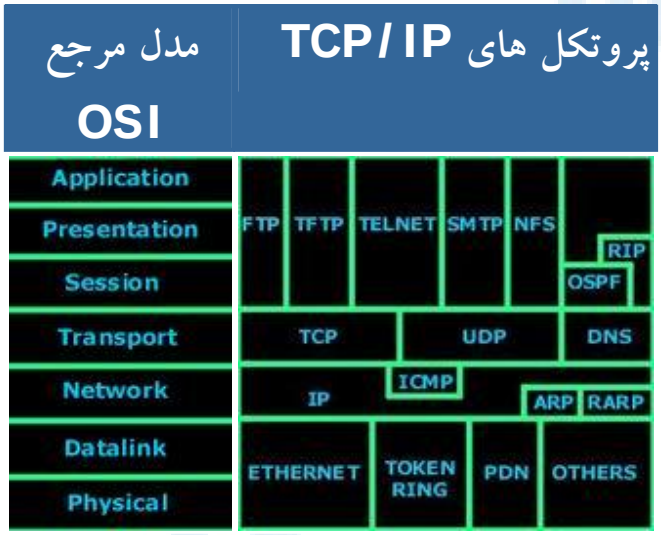
یک شبکه کامپیوتری از اتصال دو و یا چندین کامپیوتر تشکیل می گردد. شبکه های کامپیوتری در ابعاد متفاوت و با اهداف گوناگون طراحی و پیاده سازی می گردند. شبکه های Local-Area Networks (LAN) و Wide-Area Networks (WAN) دو نمونه متداول در این زمینه می باشند. در شبکه های LAN، کامپیوترهای موجود در یک ناحیه محدود جغرافیائی نظیر منزل و یا محیط کار به یکدیگر متصل می گردند. در شبکه های WAN، با استفاده از خطوط تلفن و یا مخابراتی، امواج رادیوئی و سایر گزینه های موجود، دستگاه های مورد نظر در یک شبکه به یکدیگر متصل می گردند.

شبکه های کامپیوتری چگونه تقسیم بندی می گردند ؟

شبکه های کامپیوتری را می توان بر اساس سه ویژگی متفاوت تقسیم نمود: توپولوژی، پروتکل و معماری

- **توپولوژی** ، نحوه استقرار(آرایش) هندسی یک شبکه را مشخص می نماید. bus , ring و star ، سه نمونه متداول در این زمینه می باشند.
- **پروتکل**، مجموعه قوانین لازم به منظور مبادله اطلاعات بین کامپیوترهای موجود در یک شبکه را مشخص می نماید. اکثر شبکه ها از "اترنت" استفاده می نمایند. در برخی از شبکه ها ممکن است از پروتکل Token Ring شرکت IBM استفاده گردد. پروتکل، در حقیت به منزله یک اعلامیه رسمی است که در آن قوانین و رویه های مورد نیاز به منظور ارسال ویا دریافت داده، تعریف می گردد. در صورتی که دارای دو و یا چندین دستگاه (نظیر کامپیوتر) باشیم و بخواهیم آنان را به یکدیگر مرتبط نمائیم، قطعا" به وجود یک پروتکل در شبکه نیاز خواهد بود. تاکنون صدها پروتکل با اهداف متفاوت طراحی و پیاده سازی شده است.

- TCP/IP یکی از متداولترین پروتکل ها در زمینه شبکه بوده که خود از مجموعه پروتکل هائی دیگر، تشکیل شده است. جدول زیر متداولترین پروتکل های TCP/IP را نشان می دهد. در کنار جدول فوق ، مدل مرجع OSI نیز ارائه شده است تا مشخص گردد که هر یک از پروتکل های فوق در چه لایه ای از مدل OSI کار می کنند. به موازات حرکت از پائین ترین لایه (لایه فیزیکی) به بالاترین لایه (لایه Application)، هر یک از دستگاههای مرتبط با پروتکل های موجود در هر لایه به منظور انجام پردازش های مورد نیاز ، زمانی را صرف خواهند کرد.



- OSI از کلمات Open Systems Interconnect اقتباس و یک مدل مرجع در خصوص نحوه ارسال پیام بین دو نقطه در یک شبکه مخابراتی و ارتباطی است. هدف عمده مدل OSI، ارائه راهنمائی های لازم به تولید کنندگان محصولات شبکه ای به منظور تولید محصولات سازگار با یکدیگر است. مدل OSI توسط کمیته IEEE ایجاد تا محصولات تولید شده توسط تولید کنندگان متعدد قادر به کار و یا سازگاری با یکدیگر باشند. مشکل عدم سازگاری بین محصولات تولیدشده توسط شرکت های بزرگ تجهیزات سخت افزاری زمانی آغاز گردید که شرکت HP تصمیم به ایجاد محصولات شبکه ای نمود و محصولات تولید شده توسط HP با محصولات مشابه تولید شده توسط شرکت

های دیگر نظیر IBM، سازگار نبود. مثلا" زمانی که شما چهل کارت شبکه را برای شرکت خود تهیه می نمودید، می بایست سایر تجهیزات مورد نیاز شبکه نیز از همان تولید کننده خریداری می گردید(اطمینان از وجود سازگاری بین آنان). مشکل فوق پس از معرفی مدل مرجع OSI، برطرف گردید. مدل OSI دارای هفت لایه متفاوت است که هر یک از آنان به منظور انجام عملیاتی خاصی طراحی شده اند. بالاترین لایه، لایه هفت (Application) و پائین ترین لایه، لایه یک (Physiacal) می باشد. در صورتی که قصد ارسال داده برای یک کاربر دیگر را داشته باشید، داده ها حرکت خود را از لایه هفتم شروع نموده و پس از تبدیل به سگمنت، datagram، بسته اطلاعاتی (Packet) و فریم، در نهایت در طول کابل (عموما" کابل های twisted pair) ارسال تا به کامپیوتر مقصد برسد.

- **معماری** ، به دو گروه عمده معماری که عمدتا" در شبکه های کامپیوتری استفاده می گردد ، اشاره می نماید: Peer-To-Peer و Client – Server. در شبکه های Peer-To-Peer سرویس دهنده اختصاصی وجود نداشته و کامپیوترها از طریق workgroup به منظور اشتراک فایل ها، چاپگرها و دستیابی به اینترنت، به یکدیگر متصل می گردند.
-] در شبکه های Client – Server ، سرویس دهنده و یا سرویس دهندگانی اختصاصی وجود داشته (نظیر یک کنترل کننده Domain در ویندوز) که تمامی سرویس گیرندگان به منظور استفاده از سرویس ها و خدمات ارائه شده، به آن log on می نمایند. در اکثر سازمان و موسسات از معماری Client – Server به منظور پیکربندی شبکه های کامپیوتری، استفاده می گردد.

MAC Address چیست؟

هر کامپیوتر موجود در شبـــکه به منظور ایجاد ارتباط با ســایر کامپیوترها، می بایست شناسائی و دارای یک آدرس منحصربفرد باشد . قطعا" تاکنون با آدرس های IP و یـا MAC (اقتباس شده از کلمات Media Access Control) برخورد داشته اید و شاید این سوال برای شما مطرح شده باشد که اولا" ضرورت وجود دو نوع آدرس چیست و ثانیا" جایگاه اسفاده از آنان چیست؟

MAC Address ، یک آدرس فیزیکی است در حالی که آدرس های IP ، به منزله آدرس های منطقی می باشند. آدرس های منطقی شما را ملزم می نمایند که به منـــظور پیکربندی کامپیوتر و کارت شبکه، درایورها و یا پروتکل های خاصـی را در حافـــظه مستقر نمائید (مثلا" استفاده از آدرس های IP). این وضعیت در رابطه با MAC Address صدق نخواهد کرد و اینگونه آدرس ها نیازمند درایورهای خاصی نخواهند بود ، چراکه آدرس های فوق درون تراشه کارت شبکه قرار می گیرند.

دلیل استفاده از MAC Address

هر کامپیوتر موجود در شبکه ، می بایست با استفاده از روش هائی خاص شناسائی گردد. برای شناسائی یک کامپیوتر موجود در شبکه ، صرف داشتن یک آدرس IP به تنهائی کفایت نخواهد کرد. حتما" علاقه مندید که علت این موضوع را بدانید . بدین منظور، لازم است نگاهی به مدل معروف OSI (Open Systems Interconnect) و لایه های آن داشته باشیم:

مدل OSI		
...		
Network Layer	لایه سوم	آدرس IP در این لایه قرار دارد
DataLink Layer	لایه دوم	آدرس MAC در این لایه قرار دارد
Physical Layer	لایه اول	
شبکه فیزیکی		

همانگونه که مشاهده می نمائید ، MAC Address در لایه DataLink (لایه دوم مدل OSI) قرار دارد و این لایه مسئول بررسی این موضوع خواهد بود که داده متعلق به کدامیک از کامپیوترهای موجود در شبکه است.

زمانی که یک بسته اطلاعاتی(Packet) به لایه Datalink می رسد (از طریق لایه اول)، وی آن را در اختیار لایه بالائی خود (لایه سوم) قرار خواهد داد. بنابراین ما نیازمند استفاده از روش خاصی به منظور شناسائی یک کامپیوتر قبل از لایه سوم هستیم. MAC Address، در پاسخ به نیاز فوق در نظر گرفته شده و با استقرار در لایه دوم، وظیفه شناسائی کامپیوتر قبل از لایه سوم را بر عهده دارد. تمامی ماشین های موجود بر روی یک شبکه، اقدام به بررسی بسته های اطلاعاتی نموده تا مشخص گردد که آیا MAC Address موجود در بخش "آدرس مقصد " بسته اطلاعاتی ارسالی با آدرس آنان مطابقت می نماید؟ لایه فیزیکی(لایه اول) قادر به شناخت سیگنال های الکتریکی موجود بر روی شبکه بوده و فریم هائی را تولید می نماید که در اختیار لایهDatalink گذاشته می شود. در صورت مطابقت MAC Address موجود در بخش "آدرس مقصد " بسته اطلاعاتی ارسالی با MAC Address یکی از کامپیوترهای موجود در شبکه،

کامپیوتر مورد نظر آن را دریافت و با ارسال آن به لایه سوم ، آدرس شبکه ای بسته اطلاعاتی (IP) بررسی تا این اطمینان حاصل گردد که آدرس فوق با آدرس شبکه ای که کامپیوتر مورد نظر با آن پیکربندی شده است بدرستی مطابقت می نماید.

ساختار MAC Address

یک MAC Address بر روی هر کارت شبکه همواره دارای طولی مشابه و یکسان می باشند. (شش بایت و یا ٤٨ بیت). در صورت بررسی Address MAC یک کامپیوتر که بر روی آن کارت شبکه نصب شده است، آن را با فرمت مبنای شانزده (Hex)، مشاهده خواهید دید . مثلا" MAC Address کارت شبکه موجود بر روی یک کامپیوتر می تواند به صورت زیر باشد:

مشاهده MAC Address					
استفاده از دستور IPconfig/all و مشاهده بخش Physical address :					
6A	DB	79	BA	50	00
تعریف شده توسط تولید کننده			تعریف شده توسط IEEE با توجه به RFC ۱۷۰۰		

زمانی که یک تولید کننده نظیر اینتل، کارت ها ی شبکه خود را تولید می نماید، آنان هر آدرس دلخواهی را نمی توانند برای MAC Address در نظر بگیرند. در صورتی که تمامی تولید کنندگان کارت های شبکه بخواهند بدون وجود یک ضابطه خاص، اقدام به تعریف آدرس های فوق نمایند، قطعا" امکان تعارض بین آدرس های فوق بوجود خواهد آمد. (عدم تشخیص تولید کننده کارت و وجود دو کارت شبکه از دو تولید کننده متفاوت با آدرس های یکسان). حتما" این سوال برای شما مطرح می گردد که

MAC Address توسط چه افراد و یا سازمان هائی و به چه صورت به کارت های شبکه نسبت داده می شود؟ به منظور برخورد با مشکلات فوق، گروه IEEE ، هر MAC Address را به دو بخش مساوی تقسیم که از اولین بخش آن به منظور شناسائی تولید کننده کارت و دومین بخش به تولید کنندگان اختصاص داده شده تا آنان یک شماره سریال را در آن درج نمایند.

کد تولید کنندگان بر اساس RFC-1700 به آنان نسبت داده می شود. در صورت مشاهده RFC فوق حتما" متوجه خواهید شد که برخی از تولید کنندگان دارای بیش از یک کد می باشند. علت این امر به حجم گسترده محصولات تولیدی آنان برمی گردد. با این که MAC Address در حافظه کارت شبکه ثبت می گردد، برخی از تولید کنندگان به شما این اجازه را خواهند داد که با دریافت و استفاده از یک برنامه خاص، بتوانید بخش دوم MAC Address کارت شبکه خود را تغییر دهید(شماره سریال کارت شبکه) . علت این موضوع به استفاده مجدد از سریال های استفاده شده در سایر محصولات تولید شده توسط آنان برمی گردد (تجاوز از محدود مورد نظر). در حال حاضر احتمال این که شما دو کارت شبکه را خریداری نمائید که دارای MAC Address یکسانی باشند، بسیار ضعیف و شاید هم غیرممکن باشد.

مدل مرجع OSI

OSI از کلمات **O**pen **S**ystems **I**nterconnect اقتباس و یک مدل مرجع در رابطه با نحوه ارسال پیام بین دو نقطه در یک شبکه مخابراتی و یا کامپیوتری است. هدف عمده مدل فوق، ارائه توصیه ها و راهنمائی های لازم به تولید کنندگان محصولات شبکه ای به منظور تولید محصولاتی سازگار با سایر تولید کنندگان است.

مدل OSI توسط کمیته IEEE ایجاد شده است. با استفاده از مدل فوق، محصولات تولید شده توسط تولید کنندگان مختلف امکان کار با یکدیگر را پیدا خواهند کرد (سازگاری بین محصولات). مشکل عدم سازگاری بین محصولات تولیدشده توسط شرکت های بزرگ تولید کننده تجهیزات سخت افزاری، زمانی آغاز گردید که شرکت HP تصمیم به تولید یک محصول شبکه ای نمود و این محصول با محصولات مشابه سایر شرکت ها (مثلا" IBM) سازگار نبود. با توجه به مشکل فوق، در صورتی که قصد تهیه چهل کارت شبکه برای سازمان خود را داشته باشید، می بایست سایر تجهیزات مورد نیاز شبکه را نیز از همان تولید کننده تهیه می نمودید (اطمینان از سازگاری بین آنان). مشکل فوق تا زمان ایجاد مدل مرجع OSI همچنان وجود داشت و به عنوان یک معظل بزرگ در این زمینه مطرح بود.

مدل OSI دارای هفت لایه متفاوت است که هر یک از آنان به منظور انجام عملیاتی خاص ، طراحی شده اند. بالاترین لایه، لایه هفت و پائین ترین لایه، لایه یک است. در زمان ارسال داده از یک کامپیوتر به کامپیوتر دیگر، داده ها حرکت خود را از لایه هفتم آغاز نموده و پس از تبدیل به سگمنت، دیتاگرام، بسته اطلاعاتی (Packet) و فریم، در نهایت از طریق محیط انتقال (مثلا" کابل) برای کامپیوتر مقصد ارسال می گردند.

عملکرد هر یک از لایه های مدل مرجع OSI :

- **لایه Application (لایه هفتم)**

□ ارائه سرویس های شبکه به برنامه ها(نظیر پست الکترونیکی، ارسال فایل ها و...)

□ تشخیص زمان لازم به منظور دستیابی به شبکه

- **لایه Presentation (لایه ششم)**

□ ایجاد اطمینان لازم در رابطه با قابل استفاده بودن داده برای سیستم دریافت کننده

□ فرمت داده

□ ساختمان های داده

□ توافق در رابطه با گرامر انتقال داده برای لایه Application

□ رمزنگاری داده

- **لایه Session (لایه پنجم)**

□ ا یجاد ، مدیریت و خاتمه ارتباط برقرار شده بین برنامه ها

- **لایه Transport (لایه چهارم)**

□ در ارتباط با رویکردهای متفاوت حمل داده بین کامپیوترهای میزبان

□ حمل مطمئن داده

□ ایجاد ، مدیریت و خاتمه مدارات مجازی

- تشخیص و برطرف نمودن خطاء
- تقسیم داده به فریم و نسبت دهی یک دنباله عددی مناسب به هر یک از آنان
- پروتکل های TCP، UDP و SPX در این لایه قرار دارند.

- **لایه Network (لایه سوم)**

- ارائه ارتباط و مسیر انتخابی برای دو سیستم
- حوزه روتینگ
- پاسخ به سوالات متعددی نظیر نحوه ارتباط سیستم های موجود در سگمنت های متفاوت شبکه
- آدرس های مبداء، مقصد، Subnet و تشخیص مسیر لازم
- پروتکل های IP و IPX در این لایه استفاده می گردند.

- **لایه Datalink (لایه دوم)**

- انتقال مطمئن داده از طریق محیط انتقال
- آدرس دهی فیزیکی و یا سخت افزاری (MAC)، توپولوژی شبکه
- فریم ها در این لایه قرار دارند.

- **لایه Physical (لایه اول)**

- کابل ها ، کانکتورها، ولتاژها، نرخ انتقال داده
- ارسال اطلاعات به صورت مجموعه ای از بیت ها، سیگنال های الکتریکی و اینترفیس های سخت افزاری

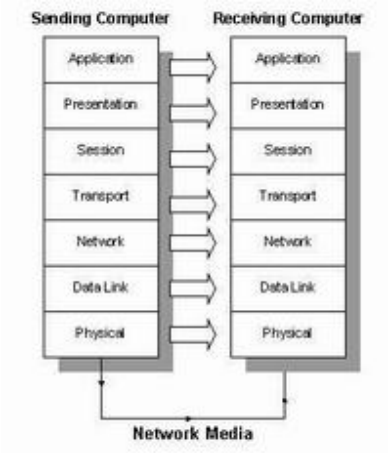
OSI

به منظور شناخت مناسب نحوه عملکرد پروتکل در شبکه می بایست با برخی از مدل های رایج شبکه که معماری شبکه را تشریح می نمایند، آشنا گردید.

مدل OSI (Open Systems Interconnection) یک مرجع مناسب در این زمینه است. این مدل در سال ۱۹۸٤ توسط ISO (یک سازمان بین المللی استاندارد سازی با بیش از ۱۳۰ عضو) ارائه گردید. در مدل فوق از هفت لایه برای تشریح فرآیندهای مربوط به ارتباطات استفاده می گردد. هریک از لایه ها مسیولیت انجام عملیات خاصی را برعهده دارند.. مدل OSI به عنوان یک مرجع و راهنما برای شناخت عملیات مربوط به ارتباطات استفاده می گردد. به منظور آشنا ئی با نحوه عملکرد یک شبکه، مطالعه مدل فوق، مفید می باشد. شکل زیر هفت لایه مدل OSI را نشان می دهد.

ارسال و دریافت اطلاعات از طریق لایه های مربوطه در کامپیوترهای فرستنده و گیرنده انجام خواهد شد. داده ها توسط یک برنامه و توسط کاربر تولید خواهند شد (نظیر یک پیام الکترونیکی). شروع ارسال داده ها از لایه Application است. در ادامه و با حرکت به سمت پایین، در هر لایه عملیات مربوطه انجام و داده هائی به بسته های اطلاعاتی اضافه خواهد شد. در آخرین لایه (لایه فیزیکی) با توجه به محیط انتقال استفاده شده، داده ها به سیگنالهای الکتریکی، پالس هائی از نور و یا سیگنالهای رادیوئی

تبدیل و از طریق کابل و یا هوا برای کامپیوتر مقصد ارسال خواهند شد. پس از دریافت داده در کامپیوتر مقصد، عملیات مورد نظر (معکوس عملیات ارسال) توسط هر یک از لایه ها انجام و در نهایت با رسیدن داده به لایه Application و بکمک یک برنامه، امکان استفاده از اطلاعات ارسالی فراهم خواهد شد. شکل زیر نحوه انجام فرآیند فوق را نشان می دهد.



لایه های OSI

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

- لایه هفت (**Application**) . این لایه با سیستم عامل و یا برنامه های کاربردی ارتباط دارد. کاربران با استفاده از نرم افزارهای کاربردی متفاوت قادر به انجام عملیات مرتبط با شبکه خواهند بود. مثلا" کاربران می توانند اقدام به ارسال فایل خواندن پیام ارسال پیام و ... نمایند.
- لایه شش (**Presentation**) . لایه فوق داده های مورد نظر خود را از لایه Application اخذ و آنها را بگونه ای تبدیل خواهد کرد که توسط سایر لایه ها قابل استفاده باشد.

- لایه پنج (**Session**) . لایه فوق مسئول ایجاد ، پشتیبانی و ارتباطات مربوطه با دستگاه دریافت کننده اطلاعات است.
- لایه چهار (**Transport**) . لایه فوق مسئول پشتیبانی کنترل جریان داده ها و و بررسی خطاء و بازیابی اطلاعات بین دستگاه های متفاوت است. کنترل جریان داده ها ، بدین معنی است که لایه فوق در صورتی که اطلاعاتی از چندین برنامه ارسال شده باشد، داده های مربوطه به هر برنامه را به یک stream آماده تبدیل تا در اختیار شبکه فیزیکی قرار داده شوند.
- لایه سه (**Network**) . در لایه فوق روش ارسال داده ها برای دستگاه گیرنده تعیین خواهد شد. پروتکل های منطقی، روتینگ و آدرس دهی در این لایه انجام خواهد شد.
- لایه دو (**Data**). در لایه فوق، پروتکل های فیزیکی به داده اضافه خواهند شد. در این لایه نوع شبکه و وضعیت بسته های اطلاعاتی (Packet) نیز تعیین می گردند.
- لایه یک (**Physical**) . لایه فوق در ارتباط مستقیم با سخت افزار بوده و خصایص فیزیکی شبکه نظیر : اتصالات، ولتاژ و زمان را مشخص می نماید.

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

پروتکل های پشته ای

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

- لایه یک (**Interface Network**) . لایه فوق، لایه های Physical و Data را ترکیب و داده های مربوط به دستگاه های موجود در یک شبکه را روت خواهد کرد.
- لایه دو (**Internet**) . لایه فوق متناظر لایه Network در مدل OSI است. پروتکل اینترنت (IP) ، با استفاده از آدرس IP (شامل یک مشخصه شبکه و یک مشخصه میزبان) ، آدرس دستگاه مورد نظر برای ارتباط را مشخص می نماید.
- لایه سه (**Transport**) . لایه فوق متناظر با لایه Transport در مدل OSI است. پروتکل TCP(Trnsport control protocol)(در لایه فوق ایفای وظیفه می نماید
- لایه چهار (**Application**) . لایه فوق متناظر با لایه های Session,Presentation و Application در مدل OSI است. پروتکل هائی نظیر FTP و SMTP در لایه فوق ایفای وظیفه می نمایند.

نحوه مبادله داده بین دو کامپیوتر

آیا تاکنون برای شما این سوال مطرح شده است که نحوه مبادله اطلاعات بین دو کامپیوتر موجود در یک شبکه به چه صورت است؟ کامپیوترهای موجود در یک شبکه به منظور مبادله اطلاعات تابع مدل مرجع OSI می باشند. مدل فوق، همانند یک دستورالعمل اجرائی بوده و عملیات لازم در زمان ارسال و یا دریافت داده را برای یک کامپیوتر مشخص می نماید. به منظور آشنائی و آنالیز فرآیند مبادله داده بین دو کامپیوتر موجود در یک شبکه به بررسی یک نمونه مثال کاربردی خواهیم پرداخت.

زمانی که یک اتومبیل در کارخانه ای تولید می گردد، یک نفر تمامی کارها را انجام نخواهد داد . تولید یک اتومبیل بر اساس یک خط تولید انجام شده و همزمان با حرکت اتومبیل در خط تولید هر شخص بخش های متفاوتی را به آن اضافه نموده و زمانی که به انتهای خط تولید می رسیم، اتومبیل مورد نظر تولید و آماده استفاده خواهد بود. وضعیت فوق در رابطه با داده ارسالی از یک کامپیوتر به کامپیوتر دیگر نیز صدق می کند. مدل OSI که توسط کمیته IEEE ایجاد شده است، قوانین لازم به منظور مبادله اطلاعات بین کامپیوترها را فراهم می نماید. بدین ترتیب و با پیروی از مجموعه رهنمودهای ارائه شده در مدل مرجع OSI، هر کامپیوتر قادر به مبادله اطلاعات با سایر کامپیوترها (صرفنظر از نوع کامپیوتر) خواهد بود. حرکت داده با دو روش متفاوت در مدل مرجع OSI انجام می شود. در سمت فرستنده (به طرف پائین)، داده ها کپسوله شده و برای کامپیوتر گیرنده ارسال می شوند. در سمت گیرنده (به طرف بالا)، داده ها از حالت کپسوله خارج شده و در نهایت در اختیار کامپیوتر گیرنده قرار داده می شوند.

ارسال داده : شکل زیرنحوه ارسال داده توسط یک کامپیوتر را نشان می دهد:

توضیحات :

- کامپیوتر موجود در شبکه، قصد ارسال داده برای کامپیوتر دیگر را دارد. در لایه Application ، رابط کاربر وجود داشته و از طریق آن کاربر با برنامه مورد نظر ارتباط برقرار می نماید.
- پس از ارسال داده از لایه Application ، داده ارسالی به ترتیب لایه های Presentation و Session را طی می نماید. هر یک از لایه های فوق اطلاعات اضافه ای را به داده اولیه اضافه نموده و در نهایت داده در اختیار لایه Transport قرار داده می شود.
- در لایه Transport ، داده به بخش های کوچکتری تقسیم و هدر TCP به آن اضافه می گردد . به داده موجود در لایه Transport ، "سگمنت" گفته می شود . هر سگمنت شماره گذاری شده تا امکان بازسازی مجدد آنان در مقصد وجود داشته باشد (انتظار داریم داده دریافتی توسط گیرنده همان داده ارسالی توسط فرستنده باشد).
- هر سگمنت در ادامه به منظور آدرس دهی شبکه (منظور آدرس دهی منطقی است) و روتینگ مناسب در اختیار لایه Network قرار داده می شود. به داده موجود در لایه Network، بسته اطلاعاتی و یا Packet گفته می شود.

لایه Network، هدر IP خود را به آن اضافه نموده و آن را برای لایه DataLink ارسال می نماید.

- در لایه DataLink به داده ئی که هم اینک شامل هدر لایه های Transport و Network است، "فریم" گفته می شود. در این لایه، هر یک از بسته های اطلاعاتی دریافتی، کپسوله شده و در یک فریم به همراه آدرس سخت افـــــزاری(آدرس MAC) کامپیوترهای فرستنده و گیرنده سازماندهی می شوند. در فریم فوق اطلاعات مربوط به LLC (نوع پروتکل ارسالی توسط لایه قبلی زمانی که به کامپیوتر مقصد می رسد)، نیز اضافه می شود. در بخش انتهائی فریم ، فیلدی با نام FCS که از کلمات Frame Check Sequence اقتباس شده است به منظور بررسی خطاء اضافه می گردد.
- در صورتی که کامپیوتر مقصد بر روی یک کامپیوتر از راه دور باشد، فریم به روتر و یا gateway به منظور مسیریابی مناسب ارسال می گردد.
- به منظور استقرار فریم بر روی شبکه می بایست اطلاعات موجود به صورت سیگنال های دیجیتال تبدیل شوند. با توجه به این که یک فریم مشتمل بر مجموعه ای از صفر و یک است، لایه Physical عملیات کپسوله نمودن ارقام موجود در فریم به یک سیگنال دیجیتال را انجام خواهد داد.
- در ابتدای فریم و به منظور انجام عملیات همزمان سازی (هماهنگ شدن دریافت کننده با فرستنده)، تعداد اندکی صفر و یک اضافه می گردد.

دریافت داده : شکل زیر نحوه دریافت داده توسط یک کامپیوتر را نشان می دهد:

توضیحات :

- کامپیوتر دریافت کننده در ابتدا به منظور هماهنگ کردن خود با کامپیوتر فرستنده در جهت خواندن سیگنال دیجیتال، تعداد محدودی از بیت ها را می خواند. پس از اتمام عملیات همزمان سازی و دریافت تمامی فریم آن را به لایه بالاتر (لایه DataLink)، ارسال می نماید.
- لایه DataLink ، در ابتدا بررسی لازم در رابطه با وجود خطاء (CRC) و یا همان Cyclic Redundancy Check را در خصوص اطلاعات دریافتی انجام خواهد داد. محاسبات فوق توسط کامپیوتر دریافت کننده انجام شده و ماحصل کار با مقدار موجود در فیلد FCS مقایسه شده و بر اساس آن تشخیص داده خواهد شد که آیا فریم دریافتی بدون بروز خطاء دریافت شده است؟ در ادامه لایه DataLink، اطلاعات اضافه و یا هدری را که توسط لایه DataLink کامپیوتر از راه دور به آن اضافه شده است را برداشته و مابقی داده را که به آن Packet اطلاق می گردد برای لایه Network ارسال می نماید.

- در لایه Network ، آدرس IP موجود در بسته اطلاعاتی با آدرس IP کامپیوتر دریافت کننده مقایسه شده و در صورت مطابقت ، هدر لایه Network و یا هدر IP از بسته اطلاعاتی برداشته شده و مابقی بسته اطلاعاتی برای لایه بالاتر (لایه Transport)، ارسال می گردد. به داده موجود در این لایه، سگمنت گفته می شود.
- سگمنت در لایه Transport پردازش و عملیات بازسازی مجدد داده دریافتی، انجام خواهد شد. در زمان بازسازی مجدد داده دریافتی توسط کامپیوتر گیرنده به فرستنده اطلاع داده می شود که وی هر یک از بخش ها را دریافت نموده است تا خللی در بازسازی مجدد داده ایجاد نگردد. با توجه به ارسال یک ACK برای فرستنده (اعلام وضعیت سگمنت دریافتی به کامپیوتر فرستنده)، از پروتکل TCP در مقابل UDP استفاده شده است. پس از انجام عملیات فوق، داده دریافتی در اختیار لایه Application گذاشته می شود. در زمان مبادله اطلاعات بین کامپیوترهای موجود در شبکه، کاربران درگیر جزئیات مسئله نشده و تمامی فرآیندهای اشاره شده به صورت اتوماتیک انجام خواهد شد.

پویش پورت ها

پویش یک پورت فرآیندی است که مهاجمان با استفاده از آن قادر به تشخیص وضعیت یک پورت بر روی یک سیستم و یا شبکه می باشند. مهاجمان با استفاده از ابزارهای متفاوت، اقدام به ارسال داده به پورت های TCP و UDP نموده و با توجه به پاسخ دریافتی قادر به تشخیص این موضوع خواهند بود که کدام پورت ها در حال استفاده بوده و از کدام پورت ها استفاده نمی گردد و اصطلاحا" آنان باز می باشند. مهاجمان در ادامه و بر اساس اطلاعات دریافتی، بر روی پورت های باز متمرکز شده و حملات خود را بر اساس آنان سازماندهی می نمایند. عملکرد مهاجمان در این رابطه مشابه سارقانی است که به منظور نیل به اهداف مخرب خود (سرقت)، درابتدا وضعیت درب ها و پنجره های منازل را بررسی نموده تا پس از آگاهی از وضعیت آنان (باز بودن و یا قفل بودن)، سرقت خود را برنامه ریزی نمایند.

TCP (Transmission Control Protocol) و(UDP (User Datagram Protocol، دو پروتـکل مهم TCP/IP می باشـند. هر یک از پروتـــکل های فوق می توانند دارای شماره پورتی بین صفر تا ٦٥،٥٣٥ باشند . بنابراین ما دارای بیش از ٦٥،٠٠٠ درب می باشیم که می بایست در رابطه با باز بودن و یا بستن هر یک از آنان تعیین تکلیف نمود (شبکه ای با بیش از ٦٥،٠٠٠ درب!). از ١٠٢٤ پورت اول TCP به منظور ارائه سرویس های استانداردی نظیر FTP,HTTP,SMTP و DNS استفاده می گردد . (پورت های خوش نام). به برخی از پورت های بالای ١٠٢٣ نیز سرویس های شناخته شده ای نسبت داده شده است، ولی اغلب این پورت ها به منظور استفاده توسط یک برنامه در دسترس می باشند.

نحوه عملکرد برنامه های پویش پورت ها

برنامه های پویش پورت ها در ابتدا اقدام به ارسال یک درخواست برای کامپیوتر هدف و بر روی هر یک از پورت ها نموده و در ادامه با توجه به نتایج بدست آمده، قادر به تشخیص وضعیت یک پورت می باشند (باز بودن و یا بسته بودن یک پورت). در صورتی که اینگونه برنامه ها با اهداف مخرب به خدمت گرفته شوند، مهاجمان قادر به تشخیص وضعیت پورت ها بر روی یک سیستم و یا شبکه کامپیوتری می شوند. آنان می توانند تهاجم خود را بگونه ای برنامه ریزی نمایند که ناشناخته باقی مانده و امکان تشخیص آنان وجود نداشته باشد. برنامه های امنیتی نصب شده بر روی یک شبکه کامپیوتری می بایست بگونه ای پیکربندی شوند که در صورت تشخیص ایجاد یک ارتباط و پویش مستمر و بدون وقفه مجموعه ای از پورت ها در یک محدوده زمانی خاص توسط یک کامپیوتر، هشدارهای لازم را در اختیار مدیریت سیستم قرار دهند. مهاجمان به منظور پویش پورت ها از دو روش عمده "آشکار" و یا " مخفی" ، استفاده می نمایند. در روش پویش آشکار ، مهاجمان در رابطه با تعداد پورت هائی که قصد بررسی آنان را دارند، دارای محدودیت خواهند بود (امکان پویش تمامی ۶۵،۵۳۵ پورت وجود ندارد). در پویش مخفی، مهاجمان از روش هائی نظیر " پویش کند " استفاده نموده تا احتمال شناسائی آنان کاهش یابد. با پویش پورت ها در یک محدوده زمانی بیشتر ، احتمال تشخیص آنان توسط برنامه های امـــنیتی نصب شده در یک شبکه کامپیوتری کاهش پیدا می نماید.

برنامه های پویش پورت ها با تنظیم فلاگ های متفاوت TCP و یا ارسال انواع متفاوتی از بسته های اطلاعاتی TCP قادر به ایجاد نتایج متفاوت و تشخیص پورت های باز بر اساس روش های مختلفی می باشند. مثلا" یک پویش مبتنی بر SYN با توجه به نتایج بدست آمده اعلام می نماید که کدام پورت باز و یا کدام پورت بسته است و یا در یک پویش مبتنی بر FIN بر اساس پاسخی که از پورت های بسته دریافت می نماید (پورت های باز پاسخی را ارسال نخواهند کرد) وضعیت یک پورت را تشخیص خواهد داد.

نحوه پیشگیری و حفاظت

مدیران شبکه می توانند با استفاده از امکانات متنوعی که در این رابطه وجود دارد از پویش پورت ها بر روی شبکه توسط مهاجمان آگاه گردند . مثلا" می توان تمامی پویش های مبتنی بر SYN را ثبت تا در ادامه امکان بررسی دقیق آنان وجود داشته باشد. (تشخیص ارسال یک بسته اطلاعاتی SYN به پورت های باز و یا بسته). به منظور افزایش ایمن سازی کامپیوتر و یا شبکه مورد نظر می توان خود راسا" اقدام به پویش پورت ها نمود . با استفاده از نرم افزارهائی نظیر NMap می توان محدوده ای از آدرس های IP و پورت های مورد نظر را بررسی نمود (شبیه سازی یک تهاجم). پس از مشخص شدن وضعیت هر یک از پورت ها می بایست اقدامات لازم حفاظتی در این خصوص را انجام داد . در صورتی که به وجود (باز بودن) یک پورت نیاز نمی باشد، می بایست آنان را غیر فعال نمود. در صورت ضرورت استفاده از یک پورت، می بایست بررسی لازم در خصوص تهدیداتی که ممکن است از جانب آن پورت متوجه سیستم و یا شبکه گردد را انجام و با نصب patch های مرتبط با آنان امکان سوء استفاده از پورت های باز را کاهش داد.

نرم افزارهای پویش پورت ها

به منظور پویش پورت ها و آگاهی از وضعیت پورت های TCP و UDP می توان از برنامه های متعددی استفاده نمود :

- Nmap (یا Network Mapper)
- FoundStone Vision
- FoundStone FPort
- FoundStone ScanLine
- Found Stone SuperScan
- FireWalls.com Port Scan (بررسی online وضعیت پورت ها)

متداولترین پورت های شبکه در ویندوز

ویندوز از یک زیرساخت جامع و پیوسته به منظور تامین طیف وسیعی از نیازها و خواسته های پیاده کنندگان وکارشناسان حرفه ای فن آوری اطلاعات، استفاده می نماید. در زیرساخت فوق برنامه های متعددی اجراء می گردد تا استفاده کنندگان اطلاعات قادر به دستیابی، آنالیز و اشتراک اطلاعات به سادگی و با سرعت بالائی باشند. محصولات سرویس دهنده شرکت مایکروسافت از تعداد زیادی پورت و پروتکل شبکه ای به منظور ارتباط بین سیستمهای سرویس گیرنده وسرویس دهنده استفاده می نمایند. در صورتی که به منظور ایمن سازی یک شبکه کامپیوتری از فایروال های خاصی و یا فیلترهای IPSec استفاده می شود، ممکن است برخی از پورت ها و پروتکل ها توسط برنامه های فوق بلاک شده و بدنبال آن امکان پاسخگوئی یک سرویس دهنده به درخواست های سرویس گیرندگان مجاز، وجود نخواهد داشت (عدم ارائه خدمات و سرویس های تعریف شده توسط یک سرویس دهنده).

برخی تعاریف اولیه

- **سیستم سرویس دهنده ویندوز** ، از محصولات متعددی نظیر خانواده نسخه های ویندوز ۲۰۰۳، سرویس دهنده Exchange 2000 ، سرویس دهنده SQL Server 2000 ، تشکیل شده است. هر یک از محصولات فوق از تعداد زیادی عناصر و سرویس های سیستم تشکیل شده اند . برخی از سرویس های سیستم در زمان راه اندازی و توسط سیستم عامل اجراء شده و برخی دیگر بر اساس تحقق شرایطی خاص ، فعالیت خود را آغاز می نمایند. هر سرویس سیستم دارای یک نام خودمانی و یک نام سرویس است. نام خودمانی، نامی است که در ابزارهای مدیریتی گرافیکی نظیر (Microsoft Management Console (MMC ، نشان داده می شوند. نام سرویس، نامی است که از آن به همراه ابزارهای خط

دستور و یا زبان های اسکریپت نویسی استفاده می گردد. هر سرویس سیستم ممکن است یک و یا چندین سرویس شبکه ای را ارائه نماید.

- **پروتکل های Application** ، پروتکل های سطح بالای شبکه بوده که از یک و یا چندین پروتکل و پورت TCP/IP استفاده می نمایند. HTTP و SMTP نمونه هائی در این زمینه می باشند.
- **پروتکل ها** ، در یک سطح پائین تر نسبت به پروتکل های Application کار می کنند . پروتکل های TCP/IP فرمت استانداردی به منظور ارتباط بین دستگاه های موجود بر روی یک شبکه را فراهم می نمایند. (پروتکل TCP/IP شامل پروتکل های دیگری نظیر TCP ، UDP و ICMP است).
- **پورت** . سرویس های سیستم با گوش دادن به پورت ها قادر به تشخیص ترافیک ورودی شبکه می باشند.

جدول زیر متداولترین پورت های شبکه در محصولات اصلی ویندوز را نشان می دهد:

System Service Name	Application protocol	Protocol	Port
Routing and Remote Access	GRE (IP protocol 47)	GRE	n/a
Routing and Remote Access	IPSec ESP (IP protocol 50)	ESP	n/a
Routing and Remote Access	IPSec AH (IP protocol 51)	AH	n/a
Simple TCP/IP Services	Echo	TCP	7
Simple TCP/IP Services	Echo	UDP	7
Simple TCP/IP Services	Discard	TCP	9

Simple TCP/IP Services	Discard	UDP	9
Simple TCP/IP Services	Daytime	TCP	13
Simple TCP/IP Services	Daytime	UDP	13
Simple TCP/IP Services	Quotd	TCP	17
Simple TCP/IP Services	Quotd	UDP	17
Simple TCP/IP Services	Chargen	TCP	19
Simple TCP/IP Services	Chargen	UDP	19
FTP Publishing Service	FTP default data	TCP	20
FTP Publishing Service	FTP control	TCP	21
Application Layer Gateway Service	FTP control	TCP	21
Telnet	Telnet	TCP	23
Simple Mail Transfer Protocol	SMTP	TCP	25
Simple Mail Transfer Protocol	SMTP	UDP	25
Exchange Server	SMTP	TCP	25
Exchange Server	SMTP	UDP	25
Windows Internet Name Service	WINS Replication	TCP	42
Windows Internet Name Service	WINS Replication	UDP	42
DNS Server	DNS	TCP	53

DNS Server	DNS	UDP	53
Internet Connection Firewall/Internet Connection Sharing	DNS	TCP	53
DHCP Server	DHCP Server	UDP	67
Internet Connection Firewall/Internet Connection Sharing	DHCP Server	UDP	67
Trivial FTP Daemon Service	TFTP	UDP	69
Windows Media Services	HTTP	TCP	80
World Wide Web Publishing Service	HTTP	TCP	80
SharePoint Portal Server	HTTP	TCP	80
Kerberos Key Distribution Center	Kerberos	TCP	88
Kerberos Key Distribution Center	Kerberos	UDP	88
Microsoft Exchange MTA Stacks	X.400	TCP	102
Microsoft POP3 Service	POP3	TCP	110
Exchange Server	POP3	TCP	110
Network News	NNTP	TCP	119

Transfer Protocol			
Windows Time	NTP	UDP	123
Windows Time	SNTP	UDP	123
Message Queuing	RPC	TCP	135
Remote Procedure Call	RPC	TCP	135
Exchange Server	RPC	TCP	135
Certificate Services	RPC	TCP	135
Cluster Service	RPC	TCP	135
Distributed File System	RPC	TCP	135
Distributed Link Tracking	RPC	TCP	135
Distributed Transaction Coordinator	RPC	TCP	135
Event Log	RPC	TCP	135
Fax Service	RPC	TCP	135
File Replication	RPC	TCP	135
Local Security Authority	RPC	TCP	135
Remote Storage Notification	RPC	TCP	135
Remote Storage Server	RPC	TCP	135
Systems Management Server 2.0	RPC	TCP	135
Terminal Services Licensing	RPC	TCP	135
Terminal	RPC	TCP	135

Services Session Directory			
Computer Browser	NetBIOS Name Resolution	UDP	137
Server	NetBIOS Name Resolution	UDP	137
Windows Internet Name Service	NetBIOS Name Resolution	UDP	137
Net Logon	NetBIOS Name Resolution	UDP	137
Systems Management Server 2.0	NetBIOS Name Resolution	UDP	137
Computer Browser	NetBIOS Datagram Service	UDP	138
Messenger	NetBIOS Datagram Service	UDP	138
Server	NetBIOS Datagram Service	UDP	138
Net Logon	NetBIOS Datagram Service	UDP	138
Distributed File System	NetBIOS Datagram Service	UDP	138
Systems Management	NetBIOS Datagram	UDP	138

Server 2.0	Service		
License Logging Service	NetBIOS Datagram Service	UDP	138
Computer Browser	NetBIOS Session Service	TCP	139
Fax Service	NetBIOS Session Service	TCP	139
Performance Logs and Alerts	NetBIOS Session Service	TCP	139
Print Spooler	NetBIOS Session Service	TCP	139
Server	NetBIOS Session Service	TCP	139
Net Logon	NetBIOS Session Service	TCP	139
Remote Procedure Call Locator	NetBIOS Session Service	TCP	139
Distributed File System	NetBIOS Session Service	TCP	139
Systems Management Server 2.0	NetBIOS Session Service	TCP	139
License Logging Service	NetBIOS Session Service	TCP	139

Exchange Server	IMAP	TCP	143
SNMP Service	SNMP	UDP	161
SNMP Trap Service	SNMP Traps Outbound	UDP	162
Local Security Authority	LDAP Server	TCP	389
Local Security Authority	LDAP Server	UDP	389
Distributed File System	LDAP Server	TCP	389
Distributed File System	LDAP Server	UDP	389
HTTP SSL	HTTPS	TCP	443
World Wide Web Publishing Service	HTTPS	TCP	443
SharePoint Portal Server	HTTPS	TCP	443
Fax Service	SMB	TCP	445
Print Spooler	SMB	TCP	445
Server	SMB	TCP	445
Remote Procedure Call Locator	SMB	TCP	445
Distributed File System	SMB	TCP	445
License Logging Service	SMB	TCP	445
Net Logon	SMB	TCP	445
Local Security Authority	IPSec ISAKMP	UDP	500
TCP/IP Print Server	LPD	TCP	515
File Server for	File Server for	TCP	548

Macintosh	Macintosh		
Windows Media Services	RTSP	TCP	554
Network News Transfer Protocol	NNTP over SSL	TCP	563
Remote Procedure Call	RPC over HTTP	TCP	593
Exchange Server	RPC over HTTP	TCP	593
Local Security Authority	LDAP SSL	TCP	636
Local Security Authority	LDAP SSL	UDP	636
Exchange Server	IMAP over SSL	TCP	993
Exchange Server	POP3 over SSL	TCP	995
Microsoft Operations Manager 2000	MOM-Encrypted	TCP	1270
Microsoft SQL Server	SQL over TCP	TCP	1433
MSSQL$UDDI	SQL over TCP	TCP	1433
Microsoft SQL Server	SQL Probe	UDP	1434
MSSQL$UDDI	SQL Probe	UDP	1434
Internet Authentication Service	Legacy RADIUS	UDP	1645
Internet Authentication Service	Legacy RADIUS	UDP	1646
Routing and Remote Access	L2TP	UDP	1701

Routing and Remote Access	PPTP	TCP	1723
Windows Media Services	MMS	TCP	1755
Windows Media Services	MMS	UDP	1755
Message Queuing	MSMQ	TCP	1801
Message Queuing	MSMQ	UDP	1801
Internet Authentication Service	RADIUS Authentication	UDP	1812
Internet Authentication Service	RADIUS Accounting	UDP	1813
SSDP Discovery Service	SSDP	UDP	1900
Message Queuing	MSMQ-DCs	TCP	2101
Message Queuing	MSMQ-RPC	TCP	2103
Message Queuing	MSMQ-RPC	TCP	2105
Message Queuing	MSMQ-Mgmt	TCP	2107
SQL Server: Downlevel OLAP Client Support	OLAP Services 7.0	TCP	2393
SQL Server: Downlevel OLAP Client Support	OLAP Services 7.0	TCP	2394
Windows Media Services	MS Theater	UDP	2460

DHCP Server	MADCAP	UDP	2535
SMS Remote Control Agent	SMS Remote Control (control)	TCP	2701
SMS Remote Control Agent	SMS Remote Control (control)	UDP	2701
SMS Remote Control Agent	SMS Remote Control (data)	TCP	2702
SMS Remote Control Agent	SMS Remote Control (data)	UDP	2702
SMS Remote Control Agent	SMS Remote Chat	TCP	2703
SMS Remote Control Agent	SMS Remote Chat	UPD	2703
SMS Remote Control Agent	SMS Remote File Transfer	TCP	2704
SMS Remote Control Agent	SMS Remote File Transfer	UDP	2704
SQL Analysis Server	SQL Analysis Services	TCP	2725
UPNP Device Host	UPNP	TCP	2869
SSDP Discovery Service	SSDP event notification	TCP	2869
Local Security Authority	Global Catalog Server	TCP	3268
Local Security Authority	Global Catalog Server	TCP	3269
Cluster Service	Cluster Services	UDP	3343
NetMeeting	Terminal	TCP	3389

Remote Desktop Sharing	Services		
Terminal Services	Terminal Services	TCP	3389
Message Queuing	MSMQ-Ping	UDP	3527
Remote Installation	BINL	UDP	4011
Local Security Authority	NAT-T	UDP	4500
SSDP Discovery Service	SSDP legacy event notification	TCP	5000
Windows Media Services	RTP	UDP	5004
Windows Media Services	RTCP	UDP	5005
ASP.NET State Service	ASP.Net Session State	TCP	42424
Microsoft Operations Manager 2000	MOM-Clear	TCP	51515

منبع : سایت مایکروسافت

پروتکل TCP/IP

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

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

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

اجزای پروتکل TCP/IP

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

پروتکل های موجود در لایه Network پروتکل TCP / IP

- پروتکل **TCP**(Transmission Control Protocol)، مهمترین وظیفه پروتکل فوق اطمینان از صحت ارسال اطلاعات است. پروتکل فوق اصطلاحا" Connection-oriented نامیده می شود. علت این امر ایجاد یک ارتباط مجازی بین کامپیوترهای فرستنده و گیرنده بعد از ارسال اطلاعات است. پروتکل هائی از این نوع، امکانات بیشتری رابه منظور کنترل خطاهای احتمالی در ارسال اطلاعات فراهم نموده ولی بدلیل افزایش بار عملیاتی سیستم کارائی آنان کاهش خواهد یافت. از پروتکل TCPبه عنوان یک پروتکل قابل اطمینان نیز یاد می شود. علت این امر ارسال اطلاعات و کسب آگاهی لازم از گیرنده اطلاعات به منظور اطمینان از صحت ارسال توسط فرستنده است. در صورتی که بسته های اطلاعاتی بدرستی دراختیار فرستنده قرار نگیرند، فرستنده مجددا" اقدام به ارسال اطلاعات می نماید.
- پروتکل **UDP**(User Datagram Protocol) . پروتکل فوق نظیر پروتکل TCP در لایه " حمل " فعالیت می نماید. UDP بر خلاف پروتکل TCP بصورت " بدون اتصال " است. بدیهی است که سرعت پروتکل فوق نسبت به TCP سریعتر بوده ولی از بعد کنترل خطاء تظمینات لازم را ارائه نخواهد داد. بهترین جایگاه استفاده از پروتکل فوق در مواردی است که برای ارسال و دریافت اطلاعات به یک سطح بالا از اطمینان، نیاز نداشته باشیم.
- پروتکل **IP**(Internet Protocol) . پروتکل فوق در لایه شبکه ایفای وظیفه کرده و مهمترین مسئولیت آن دریافت و ارسال بسته های اطلاعاتی به مقاصد درست است. پروتکل فوق با استفاده از آدرس های نسبت داده شده منطقی، عملیات روتینگ را انجام خواهد داد.

پروتکل های موجود در لایه Application پروتکل TCP/IP

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

- پروتکل **FTP**(File Transfer Protocol) . از پروتکل فوق برای تکثیر فایل های موجود بر روی یک کامپیوتر و کامپیوتر دیگر استفاده می گردد. ویندوز دارای یک برنامه خط دستوری بوده کهبه عنوان سرویس گیرنده ایفای وظیفه کرده و امکان ارسال و یا دریافت فایل ها را از یک سرویس دهنده FTP فراهم می کند.
- پروتکل **SNMP**(Protocol Simple Network Management). از پروتکل فوق به منظور اخذ اطلاعات آماری استفاده می گردد. یک سیستم مدیریتی، درخواست خود را از یک آژانس SNMP مطرح و ماحصل عملیات کار در یک MIB-Management Information Base ذخیره می گردد. MIB یک بانک اطلاعاتی بوده که اطلاعات مربوط به کامپیوترهای موجود در شبکه را در خود نگهداری می نماید. (مثلا" چه میزان فضا ی هارد دیسک وجود دارد).
- پروتکل **TelNet** . با استفاده از پروتکل فوق کاربران قادر به log on ، اجرای برنامه ها و مشاهده فایل های موجود بر روی یک کامپیوتر از راه دور می باشند. ویندوز دارای برنامه های سرویس دهنده و گیرنده جهت فعال نمودن و استفاده از پتانسیل فوق است.

- پروتکل **SMTP** (simple Mail Transfer Protocol). از پروتکل فوق برای ارسال پیام الکترونیکی استفاده می گردد.
- پروتکل **HTTP** (HyperText Transfer Protocol). پروتکل فوق مشهورترین پروتکل در این گروه بوده و از آن برای رایج ترین سرویس اینترنت یعنی وب استفاده می گردد. با استفاده از پروتکل فوق کامپیوترها قادر به مبادله فایل ها با فرمت های متفاوت (متن، تصاویر،گرافیکی، صدا، ویدئو و...) خواهند بود. برای مبادله اطلاعات با استناد به پروتکل فوق می بایست، سرویس فوق از طریق نصب سرویس دهنده وب فعال و در ادامه کاربران و استفاده کنندگان با استفاده از یک مرورگر وب قادر به استفاده از سرویس فوق خواهند بود.
- پروتکل **NNTP** (Protocol Network News Transfer). از پروتکل فوق برای مدیریت پیام های ارسالی برای گروه های خبری خصوصی و عمومی استفاده می گردد. برای عملیاتی نمودن سرویس فوق می بایست سرویس دهنده NNTPبه منظور مدیریت محل ذخیره سازی پیام های ارسالی نصب و در ادامه کاربران و سرویس گیرندگان با استفاده از برنامه ای موسوم به NewsReader از اطلاعات ذخیره شده استفاده خواهند کرد.

مدل آدرس دهی IP

علاوه بر جایگاه پروتکل ها، یکی دیگر از عناصر مهم در زیرساخت شبکه های مبتنی بر TCP/IP مدل آدرس دهی IP است. مدل انتخابی می بایست این اطمینان را بوجود آورد که اطلاعات ارسالی بدرستی به مقصد خواهند رسید.

نسخه شماره چهار IP (نسخه فعلی) از ۳۲ بیت برای آدرس دهی استفاده کرده که به منظور تسهیل در امر نمایش بصورت چهار عدد صحیح (مبنای ده) که بین آنها نقطه استفاده شده است نمایش داده می شوند.

نحوه اختصاص IP

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

Subnetting

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

کالبد شکافی آدرس های IP

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

219.27.61.137

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

11011000.00011011.00111101.10001001

همانگونه که مشاهده می گردد ، هر IP از ۳۲ بیت تشکیل می گردد. بدین ترتیب می توان حداکثر ٤،٢٩٤،٩٦٧،٢٩٦ آدرس منحصر بفرد را استفاده کرد($۲^{۳۲}$).

مثلا" آدرس ۲۵۵،۲۵۵،۲۵۵،۲۵۵ برای Broadcast (انتشار عام) استفاده می گردد.
نمایش یک IP بصورت چهار عدد (Octet) صرفا" برای راحتی کار نبوده و از آنان برای ایجاد " کلاس های IP " نیز استفاده می گردد.

هر Octet به دو بخش مجزا تقسیم می گردد: **شبکه** (Net) و **میزبان** (Host).
اولین octet نشاندهنده شبکه بوده و از آن برای مشخص نمودن شبکه ای که کامپیوتر به آن تعلق دارد، استفاده می گردد. سه بخش دیگر octet، نشاندهنده آدرس کامپیوتر موجود در شبکه است

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

- **Default Network** . آدرس IP ۰،۰،۰،۰ ، برای شبکه پیش فرض در نظر گرفته شده است. آدرس فوق برای مواردیکه کامپیوتر میزبان از آدرس خود آگاهی ندارد استفاده شده تا به پروتکل هائی نظیر DHCP اعلام نماید برای وی آدرسی را تخصیص دهد.
- **کلاس A** . کلاس فوق برای شبکه های بسیار بزرگ نظیر یک شرکت بین المللی در نظر گرفته می شود. آدرس هائی که اولین octet آنها ۱ تا ۱۲۶ باشد، کلاس A می باشند. از سه octet دیگربه منظور مشخص نمودن هر یک از کامپیوترهای میزبان استفاده می گردد. بدین ترتیب مجموع شبکه های کلاس A ، معادل ۱۲۶ و هر یک از شبکه های فوق می توانند ۱۶،۷۷۷،۲۱۴ کامپیوتر میزبان داشته باشند. (عدد فوق از طریق حاصل ۲ – $۲^{۲۴}$ بدست آمده است) .بنابراین تعداد تمام کامپیوترهای میزبان در شبکه های کلاس A معادل ۲،۱۴۷،۴۸۳،۶۴۸ ($۲^{۳۱}$) است.
در شبکه های کلاس A ، بیت با ارزش بالا در اولین octet همواره مقدار صفر را دارد.

Host (Node)	NET
24.53.107	115.

- **LoopBack** . آدرس IP ۱۲۷،۰،۰،۱ برای LoopBack در نظر گرفته شده است . کامپیوتر میزبان از آدرس فوق برای ارسال یک پیام برای خود استفاده می کند.(فرستنده و گیرنده پیام یک کامپیوتر می باشد) آدرس فوق اغلب برای تست و اشکال زدائی استفاده می گردد.
- **کلاس B** . کلاس فوق برای شبکه های متوسط در نظر گرفته می شود.(مثلا" یک دانشگاه بزرگ) آدرس هائی که اولین octet آنها ۱۲۸ تا ۱۹۱ باشد، کلاس B می باشند. در کلاس فوق از دومین octet هم برای مشخص کردن شبکه استفاده می گردد. از دو octet دیگر برای مشخص نمودن هر یک از کامپیوترهای میزبان در شبکه استفاده می گردد بدین ترتیب ۱۶،۳۸٤ ($۲^{۱٤}$) شبکه از نوع کلاس B وجود دارد. تعداد کامپیوترهای میزبان در این نوع شبکه ها(هر شبکه) معادل ٦٥،٥۳٤ (۲ – $۲^{۱٦}$) است . بنابراین تعداد تمام کامپیوترهای میزبان در شبکه های کلاس B معادل ۱،۰۷۳،۷٤۱،۸۲٤ ($۲^{۳۰}$) است در شبکه های کلاس B، اولین و دومین بیت در اولین octet به ترتیب مقدار یک و صفر را دارا می باشند.

Host (Node)	NET
53.107	145.24.

- **کلاس C** . کلاس فوق برای شبکه های کوچک تا متوسط در نظرگرفته می شود. آدرس هائی که اولین octet آنها ۱۹۲ تا ۲۲۳ باشد، کلاس (C) می باشند. در کلاس فوق از دومین و سومین octet هم برای مشخص کردن شبکه استفاده می گردد. از آخرین octet برای مشخص نمودن هر یک از کامپیوترهای میزبان در شبکه استفاده می گردد. بدین ترتیب ۲،۰۹۷،۱۵۲ ($۲^{۲۱}$) شبکه کلاس C وجود دارد.تعداد کامپیوترهای میزبان در این نوع شبکه ها(هر شبکه) معادل ۲٥٤ (۲ – $۲^{۸}$) است. بنابراین تعداد تمام کامپیوترهای میزبان در شبکه های کلاس C معادل ٥۳٦،۸۷۰،۹۱۲ ($۲^{۲۹}$) است. در شبکه های کلاس

C ، اولین ، دومین و سومین بیت در اولین octet به ترتیب مقدار یک ، یک و صفر را دارا می باشند.

Host(Node)	NET
107	195.24.53.

- **کلاس D** . از کلاس فوق برای multicasts استفاده می شود. در چنین حالتی یک گره (میزبان) بسته اطلاعاتی خود را برای یک گروه خاص ارسال می دارد. تمام دستگاه های موجود در گروه، بسته اطلاعاتی ارسال شده را دریافت خواهند کرد. (مثلا" یک روتر سیسکو آخرین وضعیت بهنگام شده خود را برای سایر روترهای سیسکو ارسال می دارد) کلاس فوق نسبت به سه کلاس قبلی دارای ساختاری کاملا" متفاوت است. اولین ، دومین ، سومین و چهارمین بیت به ترتیب دارای مقادیر یک، یک، یک و صفر می باشند.۲۸ بیت باقیمانده به منظور مشخص نمودن گروههائی از کامپیوتر بوده که پیام Multicast برای آنان در نظر گرفته می شود. کلاس فوق قادر به آدرسی دهی ۲۶۸،٤۳٥،٤٥٦ ($۲^{۲٦}$) کامپیوتر است.

Host(Node)	NET
24.53.107	224.

- **کلاس E** . از کلاس فوق برای موارد تجربی استفاده می شود. کلاس فوق نسبت به سه کلاس اولیه دارای ساختاری متفاوت است. اولین، دومین، سومین و چهارمین بیت به ترتیب دارای مقادیر یک، یک، یک و یک می باشند. ۲۸ بیت باقیمانده به منظور مشخص نمودن گروههائی از کامپیوتر بوده که پیام Multicast برای آنان در نظر گرفته می شود. کلاس فوق قادر به آدرسی دهی ۲۶۸،٤۳٥،٤٥٦ ($۲^{۲٦}$) کامپیوتر است

Host(Node)	NET
24.53.107	240.

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

255.255.255.255

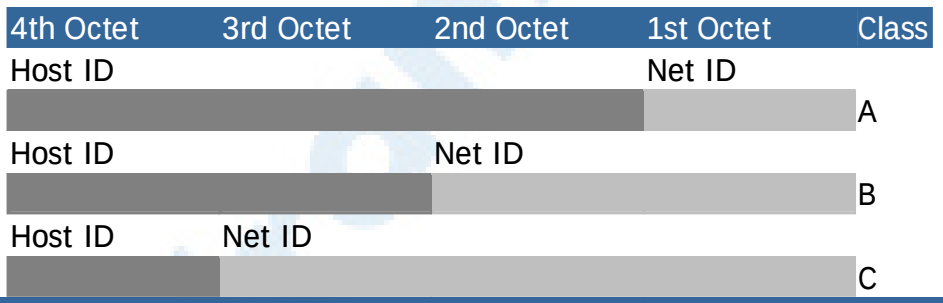
- **آدرس های رزو شده** . آدرس های IP زیربه منظور استفاده در شبکه های خصوصی (اینترانت) رزو شده اند:

10.x.x.x
172.16.x.x -
172.31.x.x
192.168.x.x

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

2b63:1478:1ac5:37ef:4e8c:75df:14cd:93f2

خلاصه :



Comments	Normal Netmask	Address Range	Network Type
For very large networks	255.0.0.0	001.x.x.x to 126.x.x.x	Class A
For medium size networks	255.255.0.0	128.1.x.x to 191.254.x.x	Class B
For small networks	255.255.255.0	192.0.1.x to 223.255.254.x	Class C
Used to support multicasting		224.x.x.x to 239.255.255.255	Class D
		240.x.x.x to 247.255.255.255	Class E

مفاهیم اولیه پروتکل TCP/IP (قسمت اول)

TCP/IP، یکی از مهمترین پروتکل های استفاده شده درشبکه های کامپیوتری است. اینترنت بعنوان بزرگترین شبکه موجود، از پروتکل فوق بمنظور ارتباط دستگاه های متفاوت استفاده می نماید. پروتکل، مجموعه قوانین لازم بمنظور قانونمند نمودن نحوه ارتباطات در شبکه های کامپیوتری است. در مجموعه مقالاتی که ارائه خواهد شد به بررسی این پروتکل خواهیم پرداخت. در این بخش مواردی همچون: فرآیند انتقال اطلاعات، معرفی و تشریح لایه های پروتکل TCP/IP و نحوه استفاده از سوکت برای ایجاد تمایز در ارتباطات، تشریح می گردد.

مقدمه

امروزه اکثر شبکه های کامپیوتری بزرگ و اغلب سیستم های عامل موجود از پروتکل TCP/IP، استفاده و حمایت می نمایند. TCP/IP ، امکانات لازم بمنظور ارتباط سیستم های غیرمشابه را فراهم می آورد.

از ویژگی های مهم پروتکل فوق، می توان به مواردی همچون : قابلیت اجراء بر روی محیط های متفاوت، ضریب اطمینان بالا ،قابلیت گسترش و توسعه آن، اشاره کرد. از پروتکل فوق، بمنظور دستیابی به اینترنت و استفاده از سرویس های متنوع آن نظیر وب و یا پست الکترونیکی استفاده می گردد. تنوع پروتکل های موجود در پشته TCP/IP و ارتباط منطقی و سیستماتیک آنها با یکدیگر، امکان تحقق ارتباط در شبکه های کامپیوتری را با اهداف متفاوت، فراهم می نماید. فرآیند برقراری یک ارتباط، شامل فعالیت های متعددی نظیر: تبدیل نام کامپیوتر به آدرس IP معادل، مشخص نمودن موقعیت کامپیوتر مقصد، بسته بندی اطلاعات، آدرس دهی و روتینگ داده ها بمنظور ارسال موفقیت آمیز به مقصد مورد نظر، بوده که توسط مجموعه پروتکل های موجود در پشته TCP/IP انجام می گیرد.

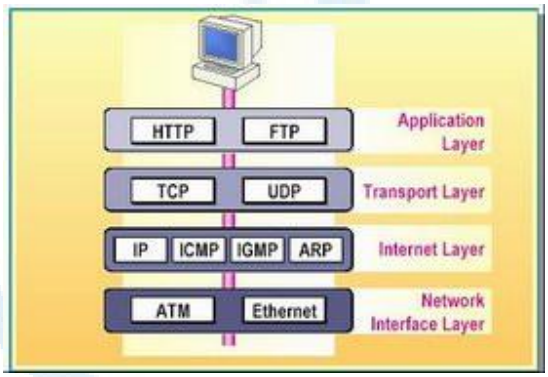
معرفی پروتکل TCP/IP

TCP/IP ، پروتکلی استاندارد برای ارتباط کامپیوترهای موجود در یک شبکه مبتنی بر ویندوز ۲۰۰۰ است. از پروتکل فوق، بمنظور ارتباط در شبکه های بزرگ استفاده می گردد. برقراری ارتباط از طریق پروتکل های متعددی که در چهارلایه مجزا سازماندهی شده اند، میسر می گردد. هر یک از پروتکل های موجود در پشته TCP/IP ، دارای وظیفه ای خاص در این زمینه (برقراری ارتباط) می باشند. در زمان ایجاد یک ارتباط، ممکن است در یک لحظه تعداد زیادی از برنامه ها، با یکدیگر ارتباط برقرار نمایند. TCP/IP، دارای قابلیت تفکیک و تمایز یک برنامه موجود بر روی یک کامپیوتر با سایر برنامه ها بوده و پس از دریافت داده ها از یک برنامه، آنها را برای برنامه متناظر موجود بر روی کامپیوتر دیگر ارسال می نماید. نحوه ارسال داده توسط پروتکل TCP/IP از محلی به محل دیگر، با فرآیند ارسال یک نامه از شـــهری به شـــهر، قابل مقایسه است.

برقراری ارتباط مبتنی بر TCP/IP ، با فعال شدن یک برنامه بر روی کامپیوتر مبدا آغاز می گردد. برنامه فوق ، داده هـای مورد نظر جهت ارسال را بگـونه ای آمـاده و فرمـــت می نماید که برای کامپیوتر مقصد قابل خواندن و استفاده باشند. (مشابه نوشتن نامه با زبانی که دریافت کننده ، قادر به مطالعه آن باشد). در ادامه آدرس کامپیوتر مقصد، به داده های مربوطه اضافه می گردد (مشابه آدرس گیرنده که بر روی یک نامه مشخص می گردد). پس از انجام عملیات فوق، داده بهمراه اطلاعات اضافی (درخواستی برای تائید دریافت در مقصد)، در طول شبکه بحرکت درآمده تا به مقصد مورد نظر برسد. عملیات فوق، ارتباطی به محیط انتقال شبکه بمنظور انتقال اطلاعات نداشته، و تحقق عملیات فوق با رویکردی مستقل نسبت به محیط انتقال، انجام خواهد شد.

لایه های پروتکل TCP/IP

TCP/IP ، فرآیندهای لازم بمنظور برقراری ارتباط را سازماندهی و در این راستا از پروتکل های متعددی در پشته TCP/IP استفاده می گردد. بمنظور افزایش کارآئی در تحقق فرآیند های مورد نظر، پروتکل ها در لایه های متفاوتی، سازماندهی شده اند. اطلاعات مربوط به آدرس دهی در انتها قرار گرفته و بدین ترتیب کامپیوترهای موجود در شبکه قادر به بررسی آن با سرعت مطلوب خواهند بود. در این راستا، صرفا" کامپیوتری که بعنوان کامپیوتر مقصد معرفی شده است، امکان باز نمودن بسته اطلاعاتی و انجام پردازش های لازم بر روی آن را دارا خواهد بود. TCP/IP ، از یک مدل ارتباطی چهار لایه بمنظور ارسال اطلاعات از محلی به محل دیگر استفاده می نماید: Application ,Internet ,Transport و Interface Network، لایه های موجود در پروتکل TCP/IP می باشند.هر یک از پروتکل های وابسته به پشته TCP/IP ، با توجه به رسالت خود ، در یکی از لایه های فوق، قرار می گیرند.



لایه Application

لایه Application ، بالاترین لایه در پشته TCP/IP است. تمامی برنامه و ابزارهای کاربردی در این لایه، با استفاده از لایه فوق، قادر به دستیابی به شبکه خواهند بود. پروتکل های موجود در این لایه بمنظور فرمت دهی و مبادله اطلاعات کاربران استفاده می گردند . HTTP و FTP دو نمونه از پروتکل ها ی موجود در این لایه می باشند.

- پروتکل Hyper text Transfer Protocol(HTTP). از پروتکل فوق، بمنظور ارسال فایل های صفحات وب مربوط به وب، استفاده می گردد.
- پروتکل File Transfer Protocol(FTP) . از پروتکل فوق برای ارسال و دریافت فایل، استفاده می گردد.

لایه Transport

لایه " حمل " ، قابلیت ایجاد نظم و ترتیب و تضمین ارتباط بین کامپیوترها و ارسال داده به لایه Application (لایه بالای خود) و یا لایه اینترنت (لایه پایین خود) را بر عهده دارد. لایه فوق ، همچنین مشخصه منحصربفردی از برنامه ای که داده را عرضه نموده است ، مشخص می نماید. این لایه دارای دو پروتکل اساسی است که نحوه توزیع داده را کنترل می نمایند.

- Transmission Control Protocol(TCP). پروتکل فوق، مسئول تضمین صحت توزیع اطلاعات است .
- User Datagram Protocol UDP). پروتکل فوق، امکان عرضه سریع اطلاعات بدون پذیرفتن مسئولیتی در رابطه با تضمین صحت توزیع اطلاعات را برعهده دارد.

لایه اینترنت

لایه "اینترنت"، مسئول آدرس دهی، بسته بندی و روتینگ داده ها، است. لایه فوق، شامل چهار پروتکل اساسی است:

- Internet Protocol(IP) . پروتکل فوق، مسئول آدرسی داده ها بمنظور ارسال به مقصد مورد نظر است.
- Address Resolation Protocol ARP). پروتکل فوق، مسئول مشخص نمودن آدرس Media Access Control MAC) آداپتور شبکه بر روی کامپیوتر مقصد است.

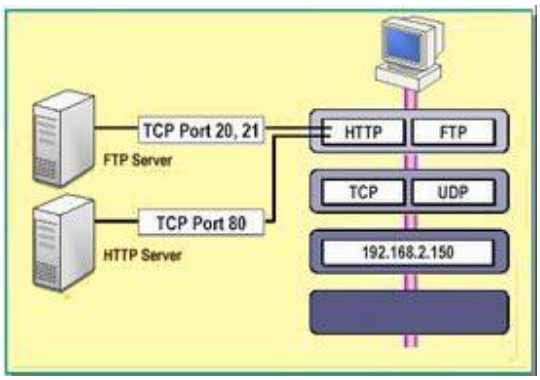
- ICMP(Internet Control Message Protocol) . پروتکل فوق، مسئول ارائه توابع عیب یابی و گزارش خطاء در صورت عدم توزیع صحیح اطلاعات است.
- IGMP(Internet Group Protocol Managemant). پروتکل فوق، مسئول مدیریت Multicasting در TCP/IP را برعهده دارد.

لایه Network Interface

لایه " اینترفیس شبکه " ، مسئول استقرار داده بر روی محیط انتقال شبکه و دریافت داده از محیط انتقال شبکه است. لایه فوق، شامل دستگاه های فیزیکی نظیر کابل شبکه و آداپتورهای شبکه است. کارت شبکه (آداپتور) دارای یک عدد دوازده رقمی مبنای شانزده (نظیر: B5-50-04-22-D4-66) بوده که آدرس MAC، نامیده می شود. لایه " اینترفیس شبکه " ، شامل پروتکل های مبتنی بر نرم افزار مشابه لایه های قبل، نمی باشد. پروتکل های Ethernet و Asynchronous Transfer Mode(ATM)، نمونه هائی از پروتکل های موجود در این لایه می باشند. پروتکل های فوق، نحوه ارسال داده در شبکه را مشخص می نمایند.

مشخص نمودن برنامه ها

در شبکه های کامپیوتری، برنامه ها ی متعددی در یک زمان با یکدیگر مرتبط می گردند. زمانیکه چندین برنامه بر روی یک کامپیوتر فعال می گردند، TCP/IP ، می بایست از روشی بمنظور تمایز یک برنامه از برنامه دیگر، استفاده نماید. بدین منظور، از یک سوکت (Socket) بمنظور مشخص نمودن یک برنامه خاص، استفاده می گردد.



آدرس IP

برقراری ارتباط در یک شبکه ، مستلزم مشخص شدن آدرس کامپیوترهای مبداء و مقصد است (شرط اولیه بمنظور برقراری ارتباط بین دو نقطه، مشخص بودن آدرس نقاط درگیر در ارتباط است). آدرس هر یک از دستگاه های درگیر در فرآیند ارتباط، توسط یک عدد منحصربفرد که IP نامیده می شود، مشخص می گردند. آدرس فوق به هریک از کامپیوترهای موجود در شبکه نسبت داده می شود. IP : ۱۰. ۱،۱،۱۰ ، نمونه ای در این زمینه است.

پورت TCP/UDP

پورت مشخصه ای برای یک برنامه و در یک کامپیوتر خاص است .پورت با یکی از پروتکل های لایه "حمل" (TCP و یا UDP) مرتبط و پورت TCP و یا پورت UDP ، نامیده می شود. پورت می تواند عددی بین صفر تا ۶۵۵۳۵ را شامل شود. پورت ها برای برنامه های TCP/IP سمت سرویس دهنده، بعنوان پورت های "شناخته شده " نامیده شده و به اعداد کمتر از ۱۰۲۴ ختم و رزو می شوند تا هیچگونه تعارض و برخوردی با سایر برنامه ها بوجود نیاید. مثلا" برنامه سرویس دهنده FTP از پورت TCP بیست و یا بیست ویک استفاده می نماید.

سوکت (Socket)

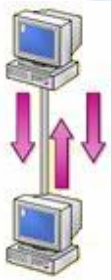
سوکت، ترکیبی از یک آدرس IP و پورت TCP ویا پورت UDP است. یک برنامه، سوکتی را با مشخص نمودن آدرس IP مربوط به کامپیوتر و نوع سرویس (TCP برای تضمین توزیع اطلاعات و یا UDP) و پورتی که نشاندهنده برنامه است، مشخص می نماید. آدرس IP موجود در سوکت، امکان آدرس دهی کامپیوتر مقصد را فراهم و پورت مربوطه ، برنامه ای را که داده ها برای آن ارسال می گردد را مشخص می نماید.

مفاهیم اولیه پروتکل TCP/IP (قسمت دوم)

در **قسمت اول**، پروتکل TCP/IP بهمراه لایه های آن معرفی گردیید. در این قسمت ، به بررسی پروتکل های موجود در TCP/IPخواهیم پرداخت.

TCP/IP ،شامل شش پروتکل اساسی(ARP، TCP,UDP,IP,ICMP,IGMP) و مجموعه ای از برنامه های کاربردی است. پروتکل های فوق، مجموعه ای از استانداردها ی لازم بمنظور ارتباط بین کامپیوترها و دستگاهها را در شبکه، فراهم می نماید. تمامی برنامه ها و سایر پروتکل ها ی موجود در پروتکل TCP/IP ، به پروتکل های شش گانه فوق مرتبط و از خدمات ارائه شده توسط آنان استفاده می نمایند. در ادامه به تشریح عملکرد و جایگاه هر یک از پروتکل های اشاره شده، خواهیم پرداخت.

پروتکل TCP : لایه Transport



TCP (Transmission Control Protocol)، یکی از پروتکل های استاندارد TCP/IP است که امکان توزیع و عرضه اطلاعات (سرویس ها) بین صرفا" دو کامپیوتر، با ضریب اعتماد بالا را فراهم می نماید. چنین ارتباطی (صرفا" بین دو نقطه)، Unicast نامیده می شود. در ارتباطات با رویکرد اتصال گرا، می بایست قبل از ارسال داده، ارتباط بین دو کامپیوتر برقرار گردد. پس از برقراری ارتباط، امکان ارسال اطلاعات برای صرفا" اتصال ایجاد شده، فراهم می گردد. ارتباطات از این نوع، بسیار مطمئن می باشند، علت این امر به تضمین توزیع اطلاعات برای مقصد مورد نظر برمی گردد.

بر روی کامپیوترمبداء، TCP داده هائی که می بایست ارسال گردند را در بسته های اطلاعاتی (Packet) سازماندهی می نماید. در کامپیوتر مقصد، TCP، بسته های اطلاعاتی را تشخیص و داده های اولیه را مجددا" ایجاد خواهد کرد.

ارسال اطلاعات با استفاده از TCP

TCP، بمنظور افزایش کارائی، بسته های اطلاعاتی را بصورت گروهی ارسال می نماید.TCP، یک عدد سریال (موقعیت یک بسته اطلاعاتی نسبت به تمام بسته اطلاعاتی ارسالی) را به هریک از بسته ها نسبت داده و از Acknowledgment بمنظور اطمینان از دریافت گروهی از بسته های اطلاعاتی ارسال شده، استفاده می نماید. در صورتیکه کامپیوتر مقصد، در مدت زمان مشخصی نسبت به اعلام وصول بسته های اطلاعاتی، اقدام ننماید، کامپیوتر مبداء ، مجددا" اقدام به ارسال اطلاعات می نماید. علاوه برافزودن یک دنباله عددی و Acknowledgment به یک بسته اطلاعاتی، TCP اطلاعات مربوط به پورت مرتبط با برنامه ها ی مبداء و مقصد را نیز به بسته اطلاعاتی اضافه می نماید. کامپیوتر مبداء، از پورت کامپیوتر مقصد بمنظور هدایت صحیح بسته های اطلاعاتی به برنامه مناسب بر روی کامپیوتر مقصد، استفاده می نماید. کامپیوتر مقصد از پورت کامپیوتر مبداء بمنظور برگرداندن اطلاعات به برنامه ارسال کننده در کامپیوتر مبداء، استفاده خواهد کرد.

هر یک از کامپیوترهائی که تمایل به استفاده از پروتکل TCP بمنظور ارسال اطلاعات دارند، می بایست قبل از مبادله اطلاعات، یک اتصال بین خود ایجاد نمایند. اتصال فوق، از نوع مجازی بوده و Session نامیده می شود. دو کامپیوتر درگیر در ارتباط، با استفاده از TCP و بکمک فرآیندی با نام: Three-Way handshake ، با یکدیگر مرتبط و هر یک پایبند به رعایت اصول مشخص شده در الگوریتم مربوطه خواهند بود.

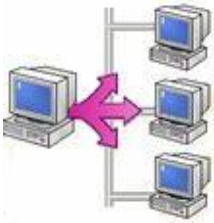
فرآیند فوق، در سه مرحله صورت می پذیرد:

مرحله اول : کامپیوتر مبداء، اتصال مربوطه را از طریق ارسال اطلاعات مربوط به Session ، مقداردهی اولیه می نماید (عدد مربوط به موقعیت یک بسته اطلاعاتی بین تمام بسته های اطلاعاتی و اندازه مربوط به بسته اطلاعاتی)

مرحله دوم : کامپیوتر مقصد، به اطلاعات Session ارسال شده، پاسخ مناسب را خواهد داد.

کامپیوتر مبداء، از شرح واقعه بکمک Acknowledgment ارسال شده توسط کامپیوتر مقصد، آگاهی پیدا خواهد کرد.

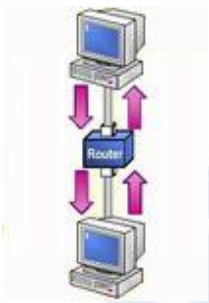
پروتکل UDP : لایه Transport



User Datagram Protocol (UDP)، پروتکلی در سطح لایه "حمل" بوده که برنامه مقصد در شبکه را مشخص نموده و از نوع بدون اتصال است. پروتکل فوق، امکان توزیع اطلاعات با سرعت مناسب را ارائه ولی در رابطه با تضمین صحت ارسال اطلاعات، سطح مطلوبی از اطمینان را بوجود نمی آورد. UDP در رابطه با داده های دریافتی توسط مقصد، به Acknowledgment نیازی نداشته و در صورت بروز اشکال و یا خرابی در داده های ارسال شده، تلاش مضاعفی بمنظور ارسال مجدد داده ها، انجام نخواهد شد. این بدان معنی است که داده هائی کمتر ارسال می گردد ولی هیچیک از داده های دریافتی و صحت تسلسل بسته های اطلاعاتی، تضمین نمی گردد. از پروتکل فوق، بمنظور انتقال اطلاعات به چندین کامپیوتر با استفاده ازBroadcast و یا Multicast، استفاده بعمل می آید . پروتکل UDP، در مواردیکه حجم اندکی از اطلاعات ارسال و یا اطلاعات دارای اهمیت بالائی نمی بانشد، نیز استفاده می گردد.

استفاده از پروتکل UDP در مواردی همچون media Multicasting Streaming،(نظیر یک ویدئو کنفرانس زنده) و یا انتشار لیستی از اسامی کامپیوترها که بمنظور ارتباطات محلی استفاده می گردند، متداول است . بمنظور استفاده از UDP ، برنامه مبداء می بایست پورت UDP خود را مشخص نماید دقیقا" مشابه عملیاتی که می بایست کامپیوتر مقصد انجام دهد. لازم به یادآوری است که پورت های UDP از پورت های TCP مجزا و متمایز می باشند (حتی اگر دارای شماره پورت یکسان باشند).

پروتکل IP : لایه Internet

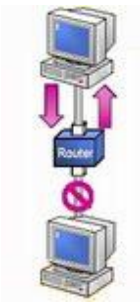


Internet Protocol (IP)، امکان مشخص نمودن محل کامپیوتر مقصد در یک شبکه ارتباطی را فراهم می نماید. IP ، یک پروتکل بدون اتصال و غیرمطمئن بوده که اولین مسئولیت آن آدرس دهی بسته های اطلاعاتی و روتینگ بین کامپیوترهای موجود در شبکه است . با اینکه IP همواره سعی در توزیع یک بسته اطلاعاتی می نماید، ممکن است یک بسته اطلاعاتی در زمان ارسال گرفتار مسائل متعددی نظیر: گم شدن، خرابی ، عدم توزیع با اولویت مناسب، تکرار در ارسال و یا تاخیر، گردند.در چنین مواردی، پروتکل IP تلاشی بمنظور حل مشکلات فوق را انجام نخواهد داد (ارسال مجدد اطلاعات درخواستی). آگاهی از وصول بسته اطلاعاتی در مقصد و بازیافت بسته های اطلاعاتی گم شده، مسئولیتی است که بر عهده یک لایه بالاتر نظیر TCP و یا برنامه ارسال کننده اطلاعات، واگذار می گردد.

عملیات انجام شده توسط IP

می توان IP را بعنوان مکانی در نظر گرفت که عملیات مرتب سازی و توزیع بسته های اطلاعاتی در آن محل، صورت می پذیرد. بسته ها ی اطلاعاتی توسط یکی از پروتکل های لایه حمل (TCP و یا UDP) و یا از طریق لایه " ایترفیس شبکه "، برای IP ارسال می گردند. اولین وظیفه IP، روتینگ بسته های اطلاعاتی بمنظور ارسال به مقصد نهائی است. هر بسته اطلاعاتی، شامل آدرس IP مبداء (فرستنده) و آدرس IP مقصد (گیرنده) می باشد. در صورتیکه IP ، آدرس مقصدی را مشخص نماید که در همان سگمنت موجود باشد، بسته اطلاعاتی مستقیما" برای کامپیوتر مورد نظر ارسال می گردد. درصورتیکه آدرس مقصد درهمان سگمنت نباشد،IP ، می بایست از یک روتر استفاده و اطلاعات را برای آن ارسال نماید.یکی دیگر از وظایف IP ، ایجاد اطمینان از عدم وجود یک بسته اطلاعاتی (بلاتکلیف !) در شبکه است. بدین منظور محدودیت زمانی خاصی در رابطه با مدت زمان حرکت بسته اطلاعاتی در طول شبکه ، در نظر گرفته می شود. عملیات فوق، توسط نسبت دادن یک مقدار TTL(Time To Live) به هر یک از بسته های اطلاعاتی صورت می پذیرد. TTL، حداکثر مدت زمانی را که بسته اطلاعاتی قادر به حرکت در طول شبکه است را مشخص می نماید(قبل از اینکه بسته اطلاعاتی کنار گذاشته شود).

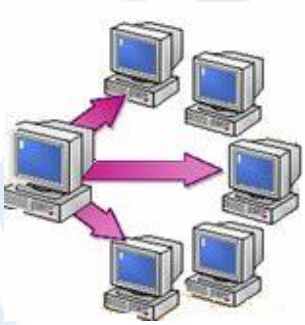
پروتکل ICMP : لایه Internet



Protocol Internet Control Message (ICMP)، امکانات لازم در خصوص اشکال زدائی و گزارش خطاء در رابطه با بسته های اطلاعاتی غیرقابل توزیع را فراهم می نماید.

با استفاده از ICMP ، کامپیوترها و روترها که از IP بمنـــظور ارتباطات استـــفاده می نمایند، قادر به گزارش خطاء و مبادله اطلاعاتی محدود در رابطه وضعیت بوجود آمده می باشند. مثلا" در صورتیکه IP ، قادر به توزیع یک بسته اطلاعاتی به مقصد مورد نظر نباشد، ICMP یک پیام مبتنی بر غیرقابل دسترس بودن را برای کامپیوتر مبداء ارسال می دارد. با اینکه پروتکل IP بمنظور انتقال داده بین روترهای متعدد استفاده می گردد، ولی ICMP به نمایندگی از TCP/IP، مسئول ارائه گزارش خطاء و یا پیام های کنترلی است. تلاش ICMP ، در این جهت نیست که پروتکل IP را بعنوان یک پروتکل مطمئن مطرح نماید، چون پیام های ICMP دارای هیچگونه محتویاتی مبنی بر اعلام وصول پیام (Acknowledgment) بسته اطلاعاتی نمی باشند. ICMP، صرفا" سعی در گزارش خطاء و ارائه فیدبک های لازم در رابطه با تحقق یک وضعیت خاص را می نماید.

پروتکل IGMP : لایه Internet

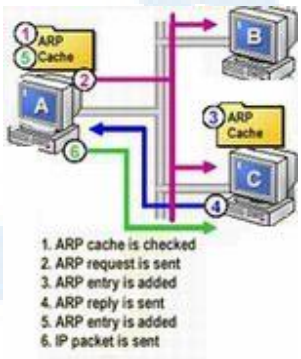


IGMP (Protocol Internet Group Managment) ، پروتکلی است که مدیریت لیست اعضاء برای Multicasting IP ، در یک شبکه TCP/IP را بر عهده دارد. IP Multicasting، فرآیندی است که بر اساس آن یک پیام برای گروهی انتخاب شده از گیرندگان که گروه multicat نامیده می شوند ؛ ارسال می گردد. IGMP لیست اعضاء را نگهداری می نماید.

مدیریت Multicasting IP

تمامی اعضاء یک گروه multicast ، به ترافیک IP هدایت شده به یک آدرس Multicast IP ، گوش داده و بسته های اطلاعاتی ارسال شده به آن آدرس را دریافت می نمایند. زمانیکه چندین کامپیوتر نیازمند دستیابی به اطلاعاتی نظیر Streaming media باشند، یک آدرس IP رزوشده برای multicasting استفاده می گردد. روترها که بمنظور پردازش multicast پیکربندی می گردند، اطلاعات را انتخاب و آنها را برای تمامی مشترکین گروه multicast ارسال (Forward) می نمایند. بمنظور رسیدن اطلاعات Multicast به گیرندگان مربوطه ، هر یک از روترهای موجود در مسیر ارتباطی می بایست، قادر به حمایت از Multicasting باشند. کامپیوترهای مبتنی بر سیستم عامل وینوز ۲۰۰۰، قادر به ارسال و دریافت IP Multicast ، می باشند.

پروتکل ARP : لایه Internet



Address Resolution Protocol (ARP)، پروتکلی است که مسئولیت مسئله " نام به آدرس" را در رابطه با بسته های اطلاعاتی خروجی (Outgoing)، برعهده دارد. ماحصل فرآیند فوق، Mapping آدرس IP به آدرسMAC (Media Access Control)، مربوطه است. کارت شبکه از آدرس MAC ، بمنظور تشخیص تعلق یک بسته اطلاعاتی به کامپیوتر مربوطه، استفاده می نمایند. بدون آدرس های MAC ، کارت های شبکه، دانش لازم در خصوص ارسال بسته های اطلاعاتی به لایه بالاتر بمنظور پردازش های مربوطه را دارا نخواهند بود.

همزمان با رسیدن بسته های اطلاعاتی به لایه IP بمنظور ارسال در شبکه، آدرس های MAC مبداء و مقصد به آن اضافه می گردد.

ARP، از جدولی خاص بمنظور ذخیره سازی آدرس های IP و MAC مربوطه، استفاده می نماید. محلی از حافظه که جدول فوق در آنجا ذخیره می گردد، Cache ARP نامیده می شود. ARP Cache هر کامپیوتر شامل mapping لازم برای کامپیوترها و روترهائی است که صرفاً بر روی یک سگمنت مشابه قرار دارند.

Physical Address Resolution

پروتکل ARP ، آدرس IP مقصد هر یک از بسته های اطلاعاتی خروجی را با ARP Cache مقایسه تا آدرس MAC مقصد مورد نظر را بدست آورد. در صورتیکه موردی پیدا گردد، آدرس MAC از Cache بازیابی می گردد. در غیر اینصورت؛ ARP درخواستی را برای کامپیوتری که مالکیت IP را برعهده دارد، Broadcast نموده و از وی می خواهد که آدرس MAC خود را اعلام نماید. کامپیوتر مورد نظر (با IP مربوطه) ، در ابتدا آدرس MAC کامپیوتر ارسال کننده درخواست را به Cache خود اضافه نموده و در ادامه پاسخ لازم را از طریق ارسال آدرس MAC خود، به متقاضی خواهد داد . زمانیکه پاسخ ARP توسط درخواست کننده، دریافت گردید، در ابتدا با استناد به اطلاعـات جدید دریافـــــتی، Cache مربوطه بهنگام و در ادامه بسته اطلاعاتی به مقصد کامپیوتر مورد نظر ارسال می گردد.

در صورتیکه مقصد یک بسته اطلاعاتی، سگمنتی دیگر باشد، ARP ، آدرس MAC را به روتر مسئول در سگمنت مربوطه، تعمیم خواهد داد (در مقابل آدرس مربوط به کامپیوتر مقصد). روتر، در ادامه مسئول یافتن آدرس MAC مقصد و یا Forwarding بسته اطلاعاتی برای روتر دیگر است.

در قسمت سوم به بررسی ، برنامه ها و ابزارهای کمکی در رابطه با پروتکل TCP/IP، خواهیم پرداخت.

مفاهیم اولیه پروتکل TCP/IP (قسمت سوم)

در **قسمت اول**، پروتکل TCP/IP بهـــمراه لایه های آن مـــــــعرفی گردید.

در **قسمت دوم**، به بررسی برخی از پروتکل های مهم موجود در پشته TCP/IP اشاره گردید. در این قسمت، به بررسی برنامه ها و ابزارهای کمکی موجود در رابطه با پروتکل TCP/IP، خواهیم پرداخت.

نسخه TCP/IP پیاد ه سازی شده در ویندوز، بهمراه خود مجموعه ای از برنامه های کاربردی را ارائه نموده است. با استفاده از برنامه های فوق ، امکان اجرای ویندوز ۲۰۰۰ بر روی یک کامپیوتر بمنظور دستیابی به مجموعه ای گسترده از اطلاعات موجود در یک شبکه ، وجود خواهد داشت. ویندوز ۲۰۰۰ ، سه گروه عمده از ابزارهای مبتنی بر TCP/IP را ارائه می نماید: برنامه های عیب یابی ، برنامه های ارتباطی و نرم افـــزارهای سمت سرویس دهنده.

در ادامه به تشریح امکانات موجود در هر گروه خواهیم پرداخت.

برنامه های عیب یابی

برنامه های عیب یابی، امکان تشخیص و برطرف نمودن مسائل مرتبط با شبکه را برای کاربران فراهم می نمایند. برخی از این ابزارها عبارتند از:

ARP . برنامه فوق، Cache مربوط به **Addreee Resolution Protocol** (ARP) را نمایش و امکان اصلاح آن را فراهم می نماید. بمنظور استفاده از برنامه فوق، کافی است ARP -a را در خط دستور تایپ و در ادامه جدول مربوط به ARP Cache ، نمایش داده می شود. با استفاده از برنامه فوق می توان یک Entry ایستا را به جدول مربوطه اضافه (arp –s ۱۵۷،۵۵،۸۵،۲۱۲ ۰۰-aa-00-62-c6-09)، و یا اقدام به حذف یک host از جدول نمود (arp -d).

Hostname . برنامه فوق، نام کامپیوتر میزبان را نمایش می دهد. برای استفاده از برنامه فوق، کافی است Hostname را در خط دستور، تایپ و نام کامپیوتر خود را مشاهده نمود.

IPConfig . برنامه فوق ، پیکربندی جاری پروتکل TCP/IP را نمایش (آدرس IP ، آدرس فیزیکی، نام کامپیوتر و ...) و امکان بهنگام سازی آن را فراهم می نماید. بمنظور آشنائی با پتانسیل های برنامه فوق ، ipcongig/help را در خط دستور تایپ تا با عملکرد این برنامه و سوئیچ های مربوطه آشنا گردید.

Nbtstat . برنامه فوق،جدول محلی اسامی NetBIOS را نمایش می دهد. جدول فوق، شامل لیستی از اسامی کامپیوترها بهمراه IP مربوطه است (mapping)

Netstat . برنامه فوق، اطلاعات مربوط به جلسه کاری (Session) پروتکل TCP/IP را نمایش می دهد.

Ping . برنامه فوق، پیکربندی و ارتباط مبتنی بر IP بین دو کامپیوتر را بررسی و تست می نماید. Ping یک درخواست ICMP را از کامپیوتر مبداء ارسال و کامپیوتر مقصد از طریق یک پاسخ ICMP به آن جواب خواهد داد .بمنظور تست ارتباط با استفاده از یک آدرس IP و یا نام یک کامپیوتر، فرمان [PING [IP_Address or Computer_Name را تایپ نمائید. بمنظور تست پیکربندی TCP/IP بر روی کامپیوتر خود، از Local Loopback استفاده نمائید. loopback Local، شامل آدرس ۱۲۷،۰،۰،۱ است.(Ping 127.0.0.1)

Tracert . برنامه فوق، ردیابی یک بسته اطلاعاتی تا رسیدن به مقصد مورد نظر را انجام می دهد.

برنامه های ارتباطی

برنامه های فوق، امکان ارتباط با مجموعه وسیعی از سیستم های مبتنی بر ویندوز و یا غیرویندوز نظیر سیستم های یونیکس، را در اختیار کاربران قرار می دهند . با اینکه این نوع از برنامه ها امکان ارسال سریع اطلاعات را فراهم می نمایند ولی با توجه به ماهیت ارسال اطلاعات توسط آنان (تمامی اطلاعات شامل اطلاعات مربوط به تائید اعتبار و هویت کاربران بصورت متن شفاف ارسال می گردد)، می بایست دقت لازم صورت پذیرد .موارد زیر نمونه هائی از برنامه های ارتباطی می باشند:

FTP . برنامه فوق، با استفاده از پروتکل TCP، اقدام به ارسال فایل بین ویندوز ۲۰۰۰ و کامپیوترهائی که بر روی آنان نرم افزار سرویس دهنده FTP نصب شده است ، می نماید.

Telnet . برنامه فوق، امکان ارتباط از راه دور به منابع شبکه موجود در کامپیوترهائی که سرویس دهنده Telnet بر روی آنان نصب شده است را فراهم می نماید.

Tftp . برنامه فوق از پروتکل UDP ، برای ارسال فایل های کوچک بین ویندوز ۲۰۰۰ و کامپیوترهائی که بر روی آنان سرویس دهنده (TFTP Trivial File Transfer Protocol) نصب شده است را فراهم می نماید.

نرم افزارهای سمت سرویس دهنده

این نوع نرم افزارها امکان چاپ و انتشار سرویس ها را برای سرویس گیرندگان مبتنی بر TCP/IP در ویندوز ۲۰۰۰ ، فراهم می نماید.

- سرویس چاپ TCP/IP . برنامه فوق ، سرویس استاندارد چاپ TCP/IP را ارائه می نماید. سرویس فوق ، امکان ارسال چاپ را برای کامپیوترهائی که بر روی آنان سیستم های عاملی بجز ویندوز ۲۰۰۰ نصب شده باشد، به چاپگر های متصل شده به یک کامپیوتر مبتنی بر ویندوز ۲۰۰۰ ، فراهم می نماید.
- سرویس های اطلاعاتی اینترنت (IIS). برنامه IIS ، نرم افزارهای سرویس دهنده متعددی نظیر وب، اخبار، پست الکترونیکی و ارسال فایل مبتنی بر

TCP/IP را در اختیار قرار می دهد. IIS، در سیستم هائی که از نسخه های Server ویندوز ۲۰۰۰ استفاده می نمایند، بصورت پیش فرض نصب می گردد. پیشنهاد می گردد در صورتیکه به عملکرد این برنامه نیازی وجود ندارد، اقدام به حذف (Uninstall) آن از روی سیستم نمود.

مثال

مثال ۱ – هدف : استفاده از برنامه Ping بمنظور اطمینان از صحت عملکرد پروتکل TCP/IP

مرحله یک : بعنوان یک کاربر مجاز ، به شبکه وارد شوید.

مرحله دو : گزینه Prompt Command را از مسیر Start | Programs | Accessories انتخاب نمائید.

مرحله سه : دستور Ping ۱۲۷،۰،۰،۱ را در پنجره مربوطه تایپ نمائید.

نتایج : پس از انجام مراحل فوق ، نتایج زیر می بایست نشان داده شود:

نتیجه یک : می بایست چهار بسته اطلاعاتی ارسال و چهار بسته اطلاعاتی دریافت و هیچگونه بسته اطلاعاتی گم نگردد. در غیر اینصورت در رابطه با نصب TCP/IP مشکلاتی وجود دارد.

نتیجه دو : در صورتیکه چهار بسته اطلاعاتی ارسال و دریافت گردد، نشاندهنده صحت عملکرد و نصب پروتکل TCP/IP است.

نتایج حاصل از اجرای برنامه Ping
C:\>ping 127.0.0.1 Pinging 127.0.0.1 with 32 bytes of data: Reply from 127.0.0.1: bytes=32 time<10ms TTL=128 Reply from 127.0.0.1: bytes=32 time<10ms TTL=128 Reply from 127.0.0.1: bytes=32

time<10ms TTL=128
Reply from 127.0.0.1: bytes=32
time<10ms TTL=128

Ping statistics for 127.0.0.1:
Packets: Sent = 4, Received = 4,
Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

مثال ۲ – هدف : استفاده از برنامه های Ping و Hostname بمنظور صحت عملکرد TCP/IP

- مرحله یک : بعنوان یک کاربر مجاز ، به شبکه وارد شوید.
- مرحله دو : گزینه Prompt Command را از مسیر | Start | Programs Accessories انتخاب نمائید.
- مرحله سه : در پنجره مربوطه ، دستور hostname را تایپ نمائید.
- مرحله چهارم : در پنجره مربوطه ، دستور Ping Computer_Name را تایپ نمائید . نام کامپیوتر ، مقدار برگردانده شده در اثر اجرای فرمان hostname است.

نتایج : پس از انجام مراحل فوق ، نتایج زیر می بایست نشان داده شود:

- نتیجه یک : نام کامپیوتر (در این رابطه هر کامپیوتر دارای نام اختصاصی مربوط به خود خواهد بود)
- نتیجه دو : آدرس IP کامپیوتر (در این رابطه هر کامپیوتر دارای آدرس IP مربوط به خود خواهد بود)

مرحله اول : مشخص نمودن نام کامپیوتر
C:\> hostname Srco

مرحله دوم : استفاده از دستور Ping بهمراه نام کامپیوتر

C:> Ping **Srco**
Pinging **Srco.Test.com** [**10.10.1.1**] with 32 bytes of data:

Reply from 10.10.1.1: bytes=32 time<10ms TTL=128
Reply from 10.10.1.1: bytes=32 time<10ms TTL=128
Reply from 10.10.1.1: bytes=32 time<10ms TTL=128
Reply from 10.10.1.1: bytes=32 time<10ms TTL=128

Ping statistics for 10.10.1.1:
Packets: Sent = 4, Received = 4, **Lost = 0 (0% loss),**
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

مفاهیم اولیه پروتکل TCP/IP (قسمت چهارم)

آنچه تاکنون گفته شده است:

قسمت اول : معرفی پروتکل TCP/IP بهمراه لایه های آن

قسمت دوم : بررسی پروتکل های موجود در TCP/IP

قسمت سوم : بررسی برنامه ها و ابزارهای کمکی در رابطه با پروتکل TCP/IP

در این قسمت به بررسی Name Resoulation ، خواهیم پرداخت. ماحصل فرآیند فوق، یافتن آدرس IP مپ (map) شده به یک نام است (در صورتیـــکه عملیات با موفقیت انجام گردد). تمامی اسامی User-friendly ، می بایست به آدرس معادل IP مربوطه مپ تا زمینه ارتباط بین دستگاههای متقاضی در یک شبکه مبتنی بر TCP/IP ، فراهم گردد.

پروتکل TCP/IP کامپیوترهای مبداء و مقصد را از طریق آدرس IP آنان، شناسائی می نماید . کاربران، تمایل بیشتری برای بخاطرسپردن و استفاده از اسامی، نسبت به اعداد(آدرس های IP) را دارند. برای آدرس دهـــــی یک کامپیوتر از انواع متفاوتی نام (user friendly names)، استفاده می گردد. ویندوز ۲۰۰۰ ، بمنظور ذخیره سازی اسامی و آدرس IP معادل آنان، از رویکردهای متفاوتی استفاده می گردد. با توجه به نوع نام استفاده شده، از یک فایل ایستا و یا پویا بمنظور ذخیره نمودن اسامی و آدرس های IP مپ شده به آنان استفاده می گردد. برخی از برنامه ها نظیر IE و FTP، قادر به استفاده از آدرس IP و یا نام برای برقراری ارتباط با مقصد مورد نظر می باشند .زمانیکه از نام استفاده می گردد، قبل از آغاز یک ارتباط از طریق پروتکل TCP/IP، از فرآیندی با نام Resolution Name استفاده تا آدرس IP کامپیوتر مورد نظر، مشخص گردد. در صورتیکه آدرس IP، مشخص شده باشد (در مقابل مشخص شدن نام)، ارتباط بلافاصله برقرارخواهد شد.

انواع نام

دو نوع نام user friendly وجود دارد: اسامی میزبان (Host) و اسامی NetBIOS . **نام میزبان** ، نامی است که به یک آدرس IP کامپیوترنسبت داده شده تا آن را بعنوان یک میزبان TCP/IP مشخص نماید. نام میزبان، می تواند دارای حداکثر ۲۵۵ کاراکتر (حروف الفبائی، کاراکترهای عددی، نقطه و hyphens) باشد. اسامی میزبان دارای اشکال متفاوتی می باشند. نام مستعار (Alias) و names Domain ، دو نمونه متداول در این زمینه می باشند. نام مستعار، نامی خاص و مرتبط شده به یک آدرس IP است. (نظیر : Tehran). یک Domain name ، بمنظور استفاده بر روی اینترنت سازماندهی و از نقطه بعنوان یک جداکننده استفاده می نماید

(مثلا" Tehran.Citys.com)

نام NetBIOS ، یک نام شانزده کاراکتری است که از آن بمنظور مشخص نمودن یک منبع NetBIOS برروی شبکه استفاده می گردد. ازیک نامNetBIOS بمنظور مشخص نمودن یک و یا مجموعه ای از کامپیوترها، استفاده میگردد.

در این راستا، صرفا" از پانزده حرف اول آن برای نام و از کاراکتر نهائی بمنظور مشخص نمودن منبع و یا سرویسی که به یک کامپیوتر اشاره می نماید، استفاده می گردد. نمونه ای از یک منبع NetBIOS ، عنصر File and Print Sharing for Microsoft Networks در شبکه های مبتنی بر ویندوز ۲۰۰۰ است . زمانیکه کامپیوتر فعالیت خود را آغاز می نماید ، عنصر فوق، یک نام منحصر بفرد NetBIOS را ریجستر(ثبت) می نماید. نام ثبت شده شامل نام کامپیوتر و کاراکتری است که بیانگر عنصر ثبت کننده است (برای در نظر گرفتن نام کامپیوتر از حداکثر پانزده حرف و برای مشخص نمودن عنصر ثبت کننده نام، از یک حرف دیگر استفاده می گردد). درویندوز ۲۰۰۰ ، نام NetBIOS ، می تواند حداکثر پانزده کاراکتر باشد. ویندوز ۲۰۰۰ ، خود نیازی به این نوع اسامی نداشته و نسخه های قبلی ویندوز نیازمند استفاده از اسامی NetBIOS بمنظور حمایت از قابلیت های شبکه ای، دارند.

Static IP mapping

زمانیکه کاربران یک نام را بمنظور برقراری ارتباط با یک کامپیوتر مقصد ، مشخص می نمایند ، پروتکل TCP/IP همچنان نیازمند یک آدرس IP برای تحقق انتقال اطلاعات است . در این راستا لازم است که نام کامپیوتر به یک آدرس IP ، مپ گردد. ماحصل عملیات فوق (mapping)، در یک جدول ایستا و یا پویا ذخیره می گردد. در صورتیکه از یک جدول ایستا استفاده گردد، نتایج مورد نظر در یکی از فایل های Hosts و یا Lmhosts ذخیره می گردند(فایل ها ی فوق، متنی می باشند). مهمترین مزیت استفاده از یک جدول ایستا ، امکان سفارشی نمودن آن با توجه به ماهیت فایل (متنی) و محل ذخیره سازی (ذخیره بر روی هر کامپیوتر) آن است. در این راستا هر یک از کاربران می توانند برای دستیابی به منابعی با فرکانس بالای دستیابی، به هر میزان که ضرورت دارد، entry در جدول فوق ثبت نمایند . بهنگام سازی جداول ایستا، یکی از چالش های اصلی در این زمینه بوده و در مواردیکه تعداد آدرس های IP مپ شده، زیاد و آدرس های فوق متناوبا" تغییر یابند، بهنگام سازی جداول ایستا مسائل خاص خود را خواهد داشت.

فایل Hosts . فایل فوق، یک فایل متنی و شامل آدرس های IP مپ شده به اسامی میزبان است . فایل فوق، دارای ویژگی های زیر است:

- می توان چندین نام میزبان را به آدرس IP مشابهی نسبت داد .در این حالت، امکان مراجعه به یک سرویس دهنده در آدرس IP : ۱۲۷،۹۱،٤٥،۱۲۱ از طریق نام حوزه Tehran.Citys.Com و یا نام مستعار Tehran وجود خواهد داشت. در این راستا، کاربران می توانند بمنظور مراجعه به سرویس دهنده از نام مستعار Tehran در مقابل نام Domain، استفاده نمایند.
- هر Entry در فایل فوق، با توجه به نوع پلات فرم، نسبت به حروف بزرگ و کوچک حساس خواهد بود. در رابطه با کامپیوترهائی که ویندوز ۲۰۰۰ و یا NT بر روی آنها نصب شده است، حساسیت فوق، وجود نخواهد داشت.

فایل LmHosts . فایل فوق، یک فایل متنی وشامل آدرس IP مپ شده به نام NetBIOS است. بخشی از فایل Lmhosts در ابتدا وارد حافظه شده و به آن اصطلاحا" NetBIOS name Cache می گویند.

mapping Dynamic IP

مهمترین مزیت جداول پویا (مسئول ذخیره سازی IP مپ شده)، بهنگام سازی اتوماتیک آنان است. در این راستا، جداول پویا از دو سرویس استفاده می نمایند: Domain Name System(DNS) و Windows Internet Neame (WINS Service). سرویس دهنده DNS و WINS عملیات مشابه ای را نظیر فایل های Hosts و Lmhosts انجام خواهند داد (بدون نیاز به پیکربندی دستی).

(Domain Name System)DNS

DNS ، روشی بمنظور نامگذاری کامپیوترها و منابع شبکه است . شبکه های مبتنی بر TCP/IP ، از بانک اطلاعاتی اسامی DNS، بمنظور یافتن کامپیوترها و سرویس ها از طریق اسامی User friendly مربوط به Domain names، استفاده می نمایند. زمانیکه کاربری نام یک Domain را در برنامه ای وارد (مشخص) می نماید، سرویس دهنده DNS ، نام مورد نظر را به IP مربوطه، map خواهد کرد .ساختار سیستم نامگذاری DNS ، بصورت سلسله مراتبی است، بدین ترتیب امکان استفاده از سیستم فوق، در شبکه های بزرگی نظیر اینترنت وجود خواهد شد. با استفاده از یک سیستم سلسله مراتبی بمنظور ایجاد اسامی Domain ، کامپیوترهائی که اسامی Domain و معادل IP مربوطه را ذخیره می نمایند، دارای mapping لازم برای صرفا" ناحیه مربوط به خود می باشند. این نوع از کامپیوترها اصطلاحا"، سرویس دهنده DNS ، نامیده شده و صرفا" پردازش های لازم برای کامپیوترهائی که در میدان عملیاتی آنان می باشد را انجام خواهند داد. زمانیکه mapping در ناحیه مربوطه تغییر نماید، سرویس دهندگان DNS مبتنی بر ویندوز ۲۰۰۰ ، بصورت اتوماتیک عملیات بهنگام سازی را انجام خواهند داد.

(Windows Internet Name Service(WINS

WINS ، یک بانـک اطلاعـــــاتی توزیعی را برای ثبـــت mapping پویای اســـامی NetBIOS استفاده شده در شبکه، ارائه می نماید. WINS، اسامی NetBIOS را بـه آدرس های IP مپ و این امکان را فراهم خواهد آورد که اســـامی NetBIOS در طول روترها، قابل استفاده باشند.

Name Resoulation در ویندوز ۲۰۰۰

Resoulation Name ، فرآیندی است که بر اساس آن مشکل یک نام برطرف و یا به یک آدرس IP مپ می گردد. زمانیکه کاربری یک نام را در یک برنامه، وارد می نماید، برنامه مشخص می نماید که نام فوق یک میزبان و یا یک نام NetBIOS است. برنامه های فعلی در ویندوز ۲۰۰۰، از فرآیند host name resolution ، استفاده می نمایند ولی برخی از برنامه های قدیمی تر نظیر برنامه هائی که مختص ویندوز NT و یا ویندوز ۹۵ ، ۹۸ طراحی شده اند، همچنان از اسامی NetBIOS استفاده می نمایند. در صورتیکه فرآیند فوق ، با موفقیت همراه نگردد، برنامه متقاضی قادر به برقراری ارتباط با مقصد مورد نظر خود نخواهد بود. در صورتیکه از یک آدرس IP استفاده می نمائید، name resolution نیاز نخواهد بود.

فرآیند Host name Resolution

آدرس IP اسامی میزبان (Host Names) ، با استفاده از فایل Host و یا بکمک سرویس دهنده DNS ، مشخص خواهد شد. فرآیند فوق ، بصورت زیر انجام خواهد شد.

- کامپیوتر A دستوری را نظیر FTP بهمراه نام کامپیوتر میزبان B ، وارد می نماید.
- کامپیوتر A ، بررسی می نماید که آیا نام مشخص شده با نام میزبان محلی مطابقت می نماید.

- در صورتیکه نام مشخص شده با نام میزبان محلی مطابقت ننماید، کامپیوتر A ، فایل میزبانان خود را (Hosts File) بمنظور آگاهی از کامپیوتر میزبان B ، جستجو می نماید. در صورتیکه نام کامپیوتر میزبان پیدا گردد، آدرس IP مپ شده به آن، برگردانده خواهد شد . پس از مشخص شدن آدرس IP ، زمینه ارتباط با کامپیوتر مورد نظر فراهم خواهد شد.
- اگر کامپیوتر A ، نام میزبان کامپیوتر B را پیدا ننماید، در ادامه یک query برای سرویس دهنده DNS ارسال می گردد. در صورتیکه نام میزبان پیدا گردد، آدرس IP نسبت داده شده به آن مشخص خواهد شد. پس از مشخص شدن آدرس IP ، زمینه ارتباط با کامپیوتر مورد نظر فراهم خواهد شد.
- درصورتیکه نام کامپیوتر میزبان در سرویس دهنده DNS پیدا نگردد، ویندوز ۲۰۰۰ ، Cache مربوط به اسامی NetBIOS را بررسی می نماید .این امر بدین علت است که ویندوز ۲۰۰۰ ، با name NetBIOS بمنزله host name ، رفتار می نماید.
- در صورتیکه Cache فوق ، شامل نام میزبان مورد نظر نباشد، یک query برای سرویس دهنده WINS ارسال می گردد.
- در صورتیکه سرویس دهنده WINS قادر به حل مشکل نام نباشد، یک پیام Broadcast بر روی شبکه ارسال می گردد.
- در صورتیکه میزبانی به پیام منتشر شده پاسخ ندهد، فایل Lmhosts بمنظور نام میزبان(NetBIOS) ، بررسی خواهد شد.

فرآیند NetBIOS Name Resolution

بصورت پیش فرض ، اسامی NetBIOS بر روی یک شبکه مبتنی بر TCP/IP کار نخواهند کرد. ویندوز ۲۰۰۰، امکان برقراری ارتباط در شبکه های مبتنی بر TCP/IP را برای سرویس گیرندگان NetBIOS ، از طریق پروتکل NetBT ، فراهم می نماید.

NetBT ، از کلمات NetBIOS over TCP/IP اقتباس شده است. پروتکل فوق، امکان برقراری ارتباط را برای برنامه های مبتنی بر NetBIOS ، توسط TCP/IP و از طریق ترجمه نام NetBIOS به یک آدرس IP، فراهم می نماید. درصورتیکه سرویس دهنده WINS برای استفاده، پیکربندی شده باشد، فرآیند NetBIOS Name Resolution ، بصورت زیر خواهد بود :

- کامپیوتر A ، دستوری نظیر Net use را بهمراه نام NetBIOS کامپیوتر B، وارد می نماید.
- کامپیوتر A ، بررسی می نماید که آیا نام مشخص شده در Cache اسامی NetBIOS ، موجود است.
- در صورتیکه نام موجود نباشد ، کامپیوتر A یک query را برای سرویس دهنده WINS ارسال می دارد.
- در صورتیکه سرویس دهنده WINS قادر به یافتن نام نباشد، کامپیوتر A از Broadcast در شبکه، استفاده می نماید.
- در صورتیکه Broadcast ، قادر به حل مشکل نام نگردد، کامپیوتر A ، فایل Lmhosts را بررسی می نماید.
- در صورتیکه روش های NetBIOS فوق، قادر به حل مشکل نام نگردند، کامپیوتر A ، فایل Hosts را بررسی می نماید.
- در نهایت ، کامپیوتر A ، یک query برای یک سرویس دهنده DNS ارسال می نماید.

در قسمت پنجم به بررسی نحوه انتقال اطلاعات خواهیم پرداخت.

مفاهیم اولیه پروتکل TCP/IP (قسمت پنجم)

آنچه تاکنون گفته شده است :

قسمت اول : معرفی پروتکل TCP/IP بهمراه لایه های آن

قسمت دوم : بررسی پروتکل های موجود در TCP/IP

قسمت سوم : بررسی برنامه ها و ابزارهای کمکی در رابطه با پروتکل TCP/IP

قسمت چهارم: بررسی Name Resoulation

در این قسمت به بررسی نحوه فرآیند انتقال اطلاعات خواهیم پرداخت.

TCP/IP ، بمنظور ارسال داده بر روی شبکه آنها را به بخش های کوچکتری با نام Packets (بسته های اطلاعاتی)، تقسیم می نماید. از بسته های اطلاعاتی، بر اساس پروتکل های مرتبط با آنان با واژه های متفاوتی یاد می گردد. تقسیم داده به بسته های اطلاعاتی امری حیاتی و ضروری است. ارسال حجم بالائی از اطلاعات در شبکه، مدت زمان زیادی طول خواهد کشید و همین امر، باعث کند شدن شبکه می گردد. در زمانیکه حجم بالائی از اطلاعات در شبکه جابجا می گردد، سایر کامپیوترهای موجود در شبکه قادر به ارسال اطلاعات نخواهند بود. در چنین حالتی، اگر در فرآیند انتقال اطلاعات اشکالی بروز نماید، می بایست تمامی اطلاعات مجدداً ارسال شوند. در مقابل، اگر بسته های اطلاعاتی کوچک بر روی شبکه ارسال گردند، انتقال آنها بسرعت انجام و محیط انتقال به مدت زیادی ، اشغال نخواهد شد. در چنین حالتی در صورتیکه هر یک از بسته های اطلاعاتی با مشکل مواجه شوند، صرفاً بسته اطلاعاتی که با مشکل مواجه شده است ، مجدداً ارسال می گردد. (در مقابل ارسال تمام اطلاعات).

زمانیکه یک بسته اطلاعاتی به لایه اینترفیس شبکه ارسال می گردد (Network interface layer)، به آن فریم (frame) می گویند. فریم ، از بخش های متفاوتی که هر یک دارای عملکرد خاص خود در جریان انتقال اطلاعات در لایه اینترفیس شبکه می باشند، تشکیل شده است.

فرآیند ارسال اطلاعات، شامل مراحل متـــعددی است (سازماندهی داده درون بسته های اطلاعاتی در کامپیوتر مبداء و بهم بستن آنان در کامپیوتر مقصد بگونه ای که شکل اولیه مجدداً ایجاد گردد). هر لایه از پروتکل **TCP/IP** ، دارای نقشی موثر در کامپیوترهای مبداء و مقصد است.

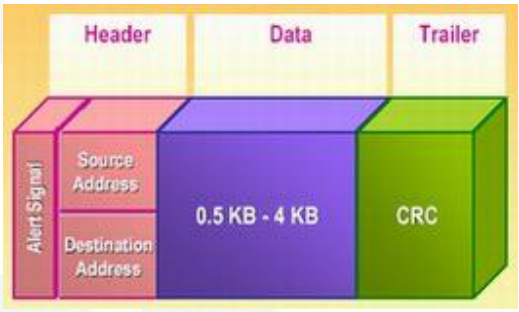
واژگان بسته های اطلاعاتی (Packets)

در هر یک از لایه های TCP/IP از بسته اطلاعاتی (packet) با اسامی متفاوتی نام برده می شود . همزمان با حرکت یک بسته اطلاعاتی از یک لایه به لایه دیگر در پروتکل TCP/IP ، هر یک از پروتکل های مربوطه ، اطلاعات اختصاصی خود را به آن اضافه می نمایند. از بسته اطلاعاتی بهمراه اطلاعات اضافه شده به آن، با اسامی فنی دیگر، یاد می گردد. این اسامی : Segment (سگمنت)، message (پیام)، datagram (دیتاگرام) و frame (فریم)، می باشند.

- **سگمنت** . سگمنت واحد انتقال اطلاعات در TCP بوده و شامل یک TCP header است که توسط Application data ، همراهی شده است.
- **پیام** . پیام ، واحد انتقال اطلاعات در پروتکل هائی نظیر ICMP,UDP,IGMP. و ARP است. پیام شامل یک header Protocol بوده که توسط Application و یا protocol data ، همراهی شده است.
- **دیتاگرام** . دیتاگرام، واحد انتقال اطلاعات در سطح لایه IP است. دیتاگرام شامل یک IP header است که توسط لایه transport ، همراهی شده است.
- **فریم**. فریم، واحد انتقال اطلاعات در سطح لایه اینترفیس شبکه است. فریم شامل یک header است که در لایه network به آن اضافه شده است که توسط داده لایه IP ، همراهی شده است.

اجزاء یک فریم

یک فریم (اصطلاحی برای یک بسته اطلاعاتی در سطح لایه شبکه) شامل سه بخش اساسی: header ، data و trailer است.



Header . اطلاعات موجود در این بخش شامل موارد زیر می باشد:

- یک سیگنال هشداردهنده مبنی بر ارسال یک بسته اطلاعاتی
- آدرس مبداء
- آدرس مقصد

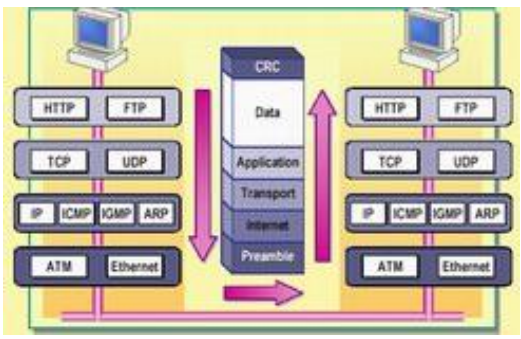
Data . در این بخش، اطلاعات واقعی ارسال شده توسط برنامه ، قرار می گیـــرد. این بخش از بسته اطلاعاتی دارای اندازه های متفاوتی است (بستگی به محدودیت اندازه تنظیم شده توسط شبکه دارد). بخش Data ، در اکثر شبکه ها از نیم کیلو بایت تا چهار کیلو بایت را می تواند شامل شود. در شبکه های اترنت ، اندازه داده تقریبا" معادل یک و نیم کیلو بایت است. با توجه به اینکه اکثر تنظیمات داده های اولیه ، بیش از چهار کیلو بایت می باشند، می بایست داده به بخش های کوچکتری با نام " بسته های اطلاعـــاتی " (packet)، تقسیم گردد. در زمان انتقال یک فایل با ظرفیت بالا، بسته های اطلاعاتی زیادی در طول شبکه منتقل خواهند شد.

Trailer . محتویات trailer ، ارتباط مستقیم به پروتکل استفاده شده در لایه اینترفیس شبکه دارد. trailer ، معمولا" شامل بخشی بمنظور بررسی خطاء بوده که Cyclical redundancy check(CRC)، نامیده می شود.CRC، عددی است که توسط یک محاسبه ریاضی بر روی بسته اطلاعتی در مبداء (فرستنده)، تولید می گردد. زمانیکه بسته اطلاعاتی به مقصد خود می رسد، مجددا" محاسبه مربوطه انجام خواهد شد. در صورتیکه نتایج بدست آمده، یکسان باشد، نشاندهنده صحت ارسال یک بسته اطلاعاتی خواهد بود . در صورتیکه ماحصل محاسبه در مقصد با نتیجه محاسبه شده در مبداء،

مغایرت داشته باشد، بدین مفهوم خواهد بود که داده در زمان انتقال، تغییر نموده است. در چنین حالتی، کامپیوتز مبداء، مجددا" داده را ارسال خواهد کرد.

جریان انتقال اطلاعات (از کامپیوتر مبداء تا کامپیوتر مقصد)

بسته های اطلاعاتی ارسال شده از یک کامپیوتر برای کامپیوتر دیگر از بین لایه های متعدد پروتکل TCP/IP عبور خواهند کرد . بموازات رسیدن یک بسته اطلاعاتی به یک لایه، پروتکل های موجود در آن، اطلاعات خاصی را به آن اضافه خواهند کرد. اطلاعات اضافه شده (ضمیمه شده) توسط هر پروتکل، شامل اطلاعاتی در رابطه با بررسی خطاء بوده که Checksum، نامیده می شود. از Checksum، بمنظور بررسی صحت ارسال اطلاعات اضافه شده در header توسط پروتکل مربوطه، در پروتکل مقصد استفاده می گردد (اطلاعات می بایست بی کم و کاست در اختیار پروتکل مقصد قرار بگیرند) .فراموش نکنیم که CRC، صحت انتقال یک بسته را بطور کامل بررسی می نماید. اطلاعات اضافه شده توسط پروتکل ها در هر لایه، بعنوان داده توسط پروتکل های لایه زیرین (پایین)، کپسوله خواهند شد. زمانیکه بسته اطلاعاتی به مقصد مورد نظر می رسد، لایه مربوطه (متناظر) یک بخش از header را برداشته و با باقی بسته اطلاعاتی بعنوان داده برخورد خواهد کرد. بسته اطلاعاتی در ادامه بسمت پروتکل های موجود در لایه بالاتر ارسال و دراختیار پروتکل مربوطه قرار خواهد گرفت. در ادامه عملکرد هر یک از لایه ها را در فرآیند انتقال اطلاعات بررسی و این موضوع را از زاویه کامپیوتر مبداء و مقصد دنبال خواهیم نمود.



لایه Application

فرآیند انتقال اطلاعات از لایه application آغاز می گردد. یک برنامه نظیر FTP، پردازش را در کامپیوتر مبداء مقدار دهی اولیه می نماید (آماده نمودن داده به فرمتی که برنامه در کامپیوتر مقصد، قادر به تشخیص آن باشد). برنامه موجود در کامپیوتر مبداء، کنترل تمامی فرآیند را برعهده خواهد داشت.

لایه Transport

از لایه Application ، داده به لایه transport منتقل می گردد. این لایه شامل پروتکل های TCP و UDP است. برنامه مورد نظر نوع پروتکل "حمل" را مشخص می نماید (TCP یا UDP). در هر دو حالت Checksum برای TCP و UDP اضافه خواهد شد.

در صورتیکه پروتکل TCP ، انتخاب گردد:

- یک دنباله عددی (number Sequence) به هر سگمنت منتقل شده ، اضافه خواهد شد.
- اطلاعات مربوط به Acknowledgment برای یک ارتباط " اتصال- گرا" ، به هر سگمنت اضافه می شود.
- شماره پورت TCP در رابطه با برنامه های مبداء و مقصد ، اضافه خواهد شد.

در صورتیکه پروتکل UDP ، انتخاب گردد:

- شماره پورت UDP در رابطه با برنامه های مبداء و مقصد ، اضافه خواهد شد.

لایه اینترنت

پس از اینکه اطلاعات "حمل " اضافه گردید ، بسته اطلاعاتی در اختیار لایه "اینترنت " قرار داده می شود. در این لایه، اطلاعات زیر به header اضافه می گردد:

- آدرس IP مبداء
- آدرس IP مقصد
- نوع پروتکل "حمل "

- مقدار checksum
- اطلاعات TTL(Time to Live)

علاوه بر اطلاعات فوق، لایه اینترنت مسئولیت بر طرف نمودن آدرس های IP مقصد به یک آدرس MAC را نیز بر عهده دارد. پروتکل ARP ، مسئول انجام عملیات فوق، است . آدرس MAC به header بسته اطلاعاتی اضافه و در ادامه بسته اطلاعاتی در اختیار لایه " اینترفیس شبکه "، قرار داده می شود.

لایه "اینترفیس شبکه "

لایه فوق، پس از دریافت یک بسته اطلاعاتی از لایه IP ، اطلاعات زیر را به آن اضافه خواهد کرد:

- یک Preamble (مقدمه) . دنباله ای از بایت ها است که ابتدای یک "فریم " را مشخص می نماید .
- یک CRC . ماحصل یک محاسبه ریاضی است که به انتهای فریم اضافه و از آن بمنظور صحت ارسال فریم، استفاده می گردد.

پس ازافزودن اطلاعات مورد نظر به فریم ها در لایه اینترفیس شبکه، در ادامه فریم ها بر روی شبکه ارسال خواهند شد.

عملیات در کامپیوتر مقصد

زمانیکه فریم ها به کامپیوتر مقصد می رسند، لایه اینترفیس شبکه ، Preamble را حذف و مقدار CRC را مجددا" محاسبه می نماید. در صورتیکه مقدار بدست آمده با مقدار محاسبه شده در مبداء، یکسان باشد در ادامه آدرس MAC مقصد، موجود بر روی فریم، بررسی می گردد. در صورتیکه آدرس MAC ، یک آدرس Broadcast و یا آدرس MAC با کامپیوتر مقصد مطابقت نماید، فریم به لایه "اینترنت "، ارسال خواهد شد. در غیر اینصورت فریم نادیده گرفته می شود. در لایه IP، مجددا" Checksum محاسبه و با مقدار محاسبه شده قبل از انتقال، مقایسه تا این اطمینان حاصل گردد که بسته اطلاعاتی در طول مسیر تغییر ننموده است. در ادامه،IP بسته اطلاعاتی را در اختیار پروتکل"حمل" ،

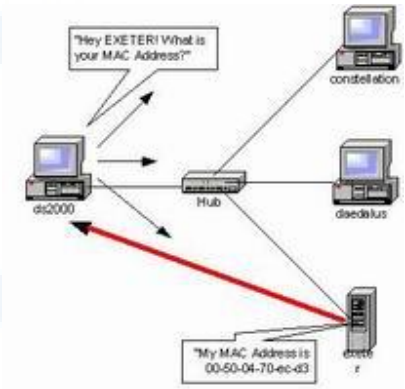
قرار می دهد (TCP یا UDP). بمنظور تصمیم گیری در رابطه با نوع پروتکل "حمل" ، از اطلاعات موجود در header IP استفاده می گردد. در لایه "حمل"، در صورتیکه بسته اطلاعاتی از TCP دریافت شده باشد، دنباله عددی (sequence number) بر روی بسته اطلاعاتی بررسی و یک acknowledgement برای TCP کامپیوتر مبداء ارسال می گردد . در ادامه از اطلاعات پورت TCP موجود در بسته اطلاعاتی استفاده تا بسته اطلاعاتی برای برنامه مربوطه در لایه Application ،ارسال گردد.

در صورتیکه UDP بسته اطلاعاتی را از لایه "اینترنت" دریافت نماید، از اطلاعات پورت UDP موجود در بسته اطلاعاتی استفاده تا آن را برای برنامه مربوطه در لایه Application ارسال نماید. (بدون ارسال یک acknowledgement برای کامپیوتر مبداء).

پس از دریافت اطلاعات توسط Appliaction ، پردازش های لازم و ضروری در ارتباط با آنها انجام خواهد شد.

DNS

DNS مسئولیت حل مشکل اسامی کامپیوترها (ترجمه نام به آدرس) در یک شبکه و مسائل مرتبط با برنامه های Winsock را بر عهده دارد. به منظور شناخت برخی از مفاهیم کلیدی و اساسی DNS ، لازم است که سیستم فوق را با سیستم دیگر نامگذاری
در شبکه های مایکروسافت(NetBIOS) مقایسه نمائیم.
قبل از عرضه ویندوز ۲۰۰۰ تمامی شبکه های مایکروسافت از مدل NetBIOS برای نامگذاری ماشین ها و سرویس ها ی موجود بر روی شبکه استفاده می کردند. NetBIOS در سال ۱۹۸۳ به سفارش شرکت IBM طراحی گردید. پروتکل فوق در ابتدا بعنوان پروتکلی در سطح لایه " حمل " ایفای وظیفه می کرد.در ادامه مجموعه دستورات NetBIOS بعنوان یک اینترفیس مربوط به لایه Session نیز مطرح تا از این طریق امکان ارتباط با سایر پروتکل ها نیز فراهم گردد. NetBEUI مهمترین و رایج ترین نسخه پیاده سازی شده در این زمینه است. NetBIOS برای شبکه های کوچک محلی با یک سگمنت طراحی شده است. پروتکل فوق بصورت Broadcast Base است . سرویس گیرندگان NetBIOS می توانند سایر سرویس گیرندگان موجود در شبکه را از طریق ارسال پیامهای Broadcast به منظور شناخت و آگاهی از آدرس سخت افزاری کامپیوترهای مقصد پیدا نمایند. شکل زیر نحوه عملکرد پروتکل فوق در یک شبکه و آگاهی از آدرس سخت افزاری یک کامپیوتر را نشان می دهد. کامپیوتر ds2000 قصد ارسال اطلاعات به کامپیوتری با نام Exeter را دارد. یک پیام Broadcast برای تمامی کامپیوترهای موجود در سگمنت ارسال خواهد شد. تمامی کامپیوترهای موجود در سگمنت مکلف به بررسی پیام می باشند. کامپیوتر Exeter پس از دریافت پیام، آدرس MAC خود را برای کامپیوتر ds2000 ارسال می نماید.



همانگونه که اشاره گردید استفاده از پروتکل فوق برای برطرف مشکل اسامی (ترجمه نام یک کامپیوتر به آدرس فیزیکی و سخت افزاری) صرفا" برای شبکه های محلی با ابعاد کوچک توصیه شده و در شبکه های بزرگ نظیر شبکه های اترنت با ماهیت Broadcast Based با مشکلات عدیده ای مواجه خواهیم شد.در ادامه به برخی از این مشکلات اشاره شده است.

- بموازات افزایش تعداد کامپیوترهای موجود در شبکه ترافیک انتشار بسته های اطلاعاتی بشدت افزایش خواهد یافت.
- پروتکل های مبتنی بر NetBIOS (نظیر NetBEUI) دارای مکانیزمهای لازم برای روتینگ نبوده و دستورالعمل های مربوط به روتینگ در مشخصه فریم بسته های اطلاعاتی NetBIOS تعریف نشده است.
- در صورتی که امکانی فراهم گردد که قابلیت روتینگ به پیامهای NetBIOS داده شود (نظیر Overlay نمودن NetBIOS بر روی پروتکل دیگر با قابلیت روتینگ ، روترها بصورت پیش فرض بسته های NetBIOS را منتشر نخواهند کرد. ماهیت BroadCast بودن پروتکل NetBIOS یکی از دو فاکتور مهم در رابطه با محدودیت های پروتکل فوق خصوصا" درشبکه های بزرگ است. فاکتور دوم ، ساختار در نظر گرفته شده برای نحوه نامگذاری است. ساختار نامگذاری در پروتکل فوق بصورت مسطح (Flat) است.

Flat NetBios NameSpace

به منظور شناخت و درک ملموس مشکل نامگذاری مسطح در NetBIOS لازم است که در ابتدا مثال هائی در این زمینه ذکر گردد. فرض کنید هر شخص در دنیا دارای یک نام بوده و صرفا" از طریق همان نام شناخته گردد. در چنین وضعیتی اداره راهنمائی و رانندگی اقدام به صدور گواهینامه رانندگی می نماید. هر راننده دارای یک شماره سریال خواهد شد. در صورتی که از اداره فوق سوالاتی نظیر سوالات ذیل مطرح گردد قطعا" پاسخگوئی به آنها بسادگی میسر نخواهد شد.

- چند نفر با نام احمد دارای گواهینامه هستند؟
- چند نفر با نام رضا دارای گواهینامه هستند؟

در چنین حالی اگر افسر اداره راهنمائی و رانندگی راننده ای را بخاطر تخلف متوقف نموده و از مرکز و بر اساس نام وی استعلام نماید که آیا " راننده ای با نام احمد قبلا" نیز مرتکب تخلف شده است یا خیر ؟" در صورتی که از طرف مرکز به وی پاسخ مثبت داده شود افسر مربوطه هیچگونه اطمینانی نخواهد داشت که راننده در مقابل آن همان احمد متخلف است که قبلا" نیز تخلف داشته است.

یکی از روش های حل مشکل فوق، ایجاد سیستمی است که مسئولیت آن ارائه نام بصورت انحصاری و غیرتکراری برای تمامی افراد در سطح دنیا باشد. در چنین وضعیتی افسر اداره راهنمائی و رانندگی در برخورد با افراد متخلف دچار مشکل نشده و همواره این اطمینان وجود خواهد داشت که اسامی بصورت منحصر بفرد استفاده شده است. در چنین سیستمی چه افراد و یا سازمانهائی مسئله عدم تکرار اسامی را کنترل و این اطمینان را بوجود خواهند آورند که اسامی بصورت تکراری در سطح دنیا وجود نخواهد داشت؟. بهرحال ساختار سیستم نامگذاری می بایست بگونه ای باشد که این اطمینان را بوجود آورد که نام انتخاب شده قبلا" در اختیار دیگری قرار داده نشده است. در عمل پیاده

سازی اینچنین سیستم هائی غیر ممکن است.مثال فوق محدودیت نامگذاری بصورت مسطح را نشان می دهد.

سیستم نامگذاری بر اساس NetBIOS بصورت مسطح بوده و این بدان معنی است که هر کامپیوتر بر روی شبکه می بایست دارای یک نام متمایز از دیگران باشد. در صورتی که دو کامپیوتر موجود بر روی شبکه های مبتنی بر NetBIOS دارای اسامی یکسانی باشند پیامهای ارسالی از یک کامپیوتر به کامپیوتر دیگر که دارای چندین نمونه (نام تکراری) در شبکه است، می تواند باعث بروز مشکلات در شبکه و عدم رسیدن پیام ارسال شده به مقصد درست خود باشد.

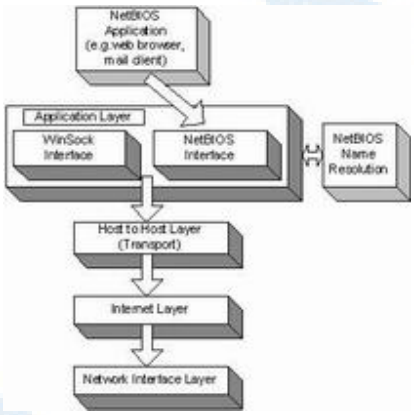
اینترفیس های NetBIOS و WinSock

DNS مسائل فوق را بسادگی برطرف نموده است. سیستم فوق از یک مدل سلسله مراتبی برای نامگذاری استفاده کرده است . قبل از پرداختن به نحوه عملکرد و جزئیات سیستم DNS لازم است در ابتدا با نحوه دستیابی برنامه ها به پروتکل های شبکه و خصوصا" نحوه ارتباط آنها با پروتکل TCP/IP آشنا شویم. برنامه های با قابلیت اجراء بر روی شبکه هائی با سیستم های عامل مایکروسافت، با استفاده از دو روش متفاوت با پروتکل TCP/IP مرتبط می گردنند.

- اینترفیس سوکت های ویندوز (WinSock)
- اینترفیس NetBIOS

اینترفیس های فوق یکی از مسائل اساسی در نامگذاری و ترجمه اسامی در شبکه های مبتنی بر TCP/IP را به چالش می کشانند.برنامه های نوشته شده که از اینترفیس NetBIOS استفاده می نمایند از نام کامپیوتر مقصد بعنوان " نقطه آخر" برای ارتباطات استفاده می نمایند در چنین مواردی برنامه های NetBIOS صرفا" مراقبت های لازم را در خصوص نام کامپیوتر مقصد به منظور ایجاد یک session انجام خواهند داد. در حالیکه پروتکل های TCP/IP)IP,TCP) هیچگونه آگاهی از اسامی کامپیوترهای

NetBIOS نداشته و در تمامی موارد مراقبت های لازم را انجام نخواهند داد. به منظور حل مشکل فوق(برنامه هائی که از NetBIOS بکمک اینترفیس NetBIOS با پروتکل TCP/IP مرتبط خواهند شد) از اینترفیس netBT و یا NetBIOS over TCP/IP استفاده می نمایند. زمانیکه درخواستی برای دستیابی به یک منبع در شبکه از طریق یک برنامه با اینترفیس NetBIOS ارائه می گردد و به لایه Application می رسد از طریق اینترفیس NetBT با آن مرتبط خواهد شد.در این مرحله نام NetBIOS ترجمه و به یک IP تبدیل خواهد شد. زمانیکه نام NetBIOS کامپیوتر به یک آدرس فیزیکی ترجمه می گردد درخواست مربوطه می تواند لایه های زیرین پروتکل TCP/IP را طی تا وظایف محوله دنبال گردد. شکل زیر نحوه انجام عملیات فوق را نشان می دهد.



اینترفیس Winsock

اغلب برنامه هائی که براساس پروتکل TCP/IP نوشته می گردند، از اینترفیس Winsock استفاده می نمایند. این نوع برنامه ها نیازمند آگاهی از نام کامپیوتر مقصد برای ارتباط نبوده و با آگاهی از آدرس IP کامپیوتر مقصد قادر به ایجاد یک ارتباط خواهند بود.

کامپیوترها جهت کار با اعداد (خصوصا" IP) دارای مسائل و مشکلات بسیار ناچیزی می باشند.در صورتی که انسان در این رابطه دارای مشکلات خاص خود است . قطعا" بخاطر سپردن اعداد بزرگ و طولانی برای هر شخص کار مشکلی خواهد بود. هر یک از ما طی روز به وب سایت های متعددی مراجعه و صرفا" با تایپ آدرس مربوطه که بصورت یک نام خاص است (www.test.com) از امکانات سایت مربوطه بهره مند می گردیم. آیا طی این نوع ملاقات ها ما نیازمند آگاهی از آدرس IP سایت مربوطه بوده ایم؟ بهرحال بخاطر سپردن اسامی کامپیوترها بمراتب راحت تر از بخاطر سپردن اعداد (کد) است. از آنجائیکه برنامه های Winsock نیازمند آگاهی از نام کامپیوتر و یا Host Name نمی باشند می توان با رعایت تمامی مسائل جانبی از روش فوق برای ترجمه اسامی استفاده کرد.فرآیند فوق را ترجمه اسامی(**Host Name Resoulation**) می گویند.

موارد اختلاف بین NetBIOS و WinSock

برنامه های مبتنی بر NetBIOS می بایست قبل از ایجاد ارتباط با یک کامپیوتر، نام NetBIOS را به یک IP ترجمه نمایند.(قبل از ایجاد ارتباط نام NetBIOS به IP تبدیل خواهد شد.) در برنامه های مبتنی بر WinSock می توان از نام کامپیوتر (Host name) در مقابل IP استفاده کرد. قبل از عرضه ویندوز ۲۰۰۰ تمامی شبکه های کامپیوتری که توسط سیستم های عامل ویندوز پیاده سازی می شدند از NetBIOS استفاده می کردند. بهمین دلیل در گذشته زمان زیادی صرف ترجمه اسامی می گردید. ویندوز وابستگی به NetBIOS نداشته و در مقابل از سیستم DNS استفاده می نماید.

DNS NameSpace

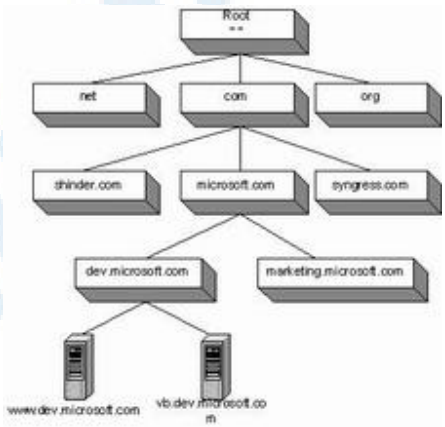
همانگونه که اشاره گردید DNS از یک ساختار سلسله مراتبی برای سیستم نامگذاری خود استفاده می نماید.

با توجه به ماهیت سلسله مراتبی بودن ساختار فوق، چندین کامپیوتر می توانند دارای اسامی یکسان بر روی یک شبکه بوده و هیچگونه نگرانی از عدم ارسال پیام ها وجود نخواهد داشت. ویژگی فوق درست نقطه مخالف سیستم نامگذاری NetBIOS است.

در مدل فوق قادر به انتخاب دو نام یکسان برای

دو کامپیوتر موجود بر روی یک شبکه یکسان نخواهیم نبود.

بالاترین سطح در DNS با نام Root Domain نامیده شده و اغلب بصورت یک "." و یا یک فضای خالی "" نشان داده می شود. بلافاصله پس از ریشه با اسامی موجود در دامنه بالاترین سطح (Top Level) برخورد خواهیم کرد. دامنه های . Com , .net , .edu , .org نمونه هائی از این نوع می باشند. سازمانهائی که تمایل به داشتن یک وب سایت بر روی اینترنت دارند، می بایست یک دامنه را که بعنوان عضوی از اسامی حوزه Top Level می باشد را برای خود اختیار نماید. هر یک از حوزه های سطح بالا دارای کاربردهای خاصی می باشند. مثلاً" سازمان های اقتصادی در حوزه .com و موسسات آموزشی در حوزه .edu و ... domain خود را ثبت خواهند نمود.شکل زیر ساختار سلسله مراتبی DNS را نشان می دهد.



در هر سطح از ساختار سلسله مراتبی فوق می بایست اسامی با یکدیگر متفاوت باشد. مثلاً" نمی توان دو حوزه .com و یا دو حوزه .net را تعریف و یا دو حوزه Microsoft.com در سطح دوم را داشته باشیم .استفاده از اسامی تکراری در سطوح

متفاوت مجاز بوده و بهمین دلیل است که اغلب وب سایت ها دارای نام www می باشند.

حوزه های Top Level و Second level تنها بخشهائی از سیستم DNS می باشند که می بایست بصورت مرکزی مدیریت و کنترل گردنند. به منظور ریجستر نمودن دامنه مورد نظر خود می بایست با سازمان و یا شرکتی که مسئولیت ریجستر نمودن را برعهده دارد ارتباط برقرار نموده و از آنها درخواست نمود که عملیات مربوط به ریجستر نمودن دامنه مورد نظر ما را انجام دهند. در گذشته تنها سازمانی که دارای مجوز لازم برای ریجستر نمودن حوزه های سطح دوم را در اختیار داشت شرکت NSI)Network Solutions Intcorporated) بود. امروزه امتیاز فوق صرفا" در اختیار شرکت فوق نبوده و شرکت های متعددی اقدام به ریجستر نمودن حوزه ها می نمایند.

مشخصات دامنه و اسم Host

هر کامپیوتر در DNS بعنوان عضوی از یک دامنه در نظر گرفته می شود. به منظور شناخت و ضرورت استفاده از ساختار سلسله مراتبی بهمراه DNS لازم است در ابتدا با FQDN آشنا شویم .

معرفی Fully(Qualified Domain Names FQDN)

یک FQDN محل یک کامپیوتر خاص را در DNS مشخص خواهد نمود. با استفاده از FQDN می توان بسادگی محل کامپیوتر در دامنه مربوطه را مشخص و به آن دستیابی نمود. FQDN یک نام ترکیبی است که در آن نام ماشین (Host) و نام دامنه مربوطه قرار خواهد گرفت . مثلا" اگر شرکتی با نام TestCorp در حوزه سطح دوم دامنه خود را ثبت نماید (TestCorp.com) در صورتی که سرویس دهنده وب بر روی TestCorp.com اجراء گردد می توان آن را www نامید و کاربران با استفاده از www.testCorp.com به آن دستیابی پیدا نمایند.

دقت داشته باشید که www از نام FQDN مثال فوق نشاندهنده یک شناسه خدماتی نبوده و صرفا" نام host مربوط به ماشین مربوطه را مشخص خواهد کرد. یک نام FQDN از دو عنصر اساسی تشکیل شده است:

- Label : شامل نام حوزه و یا نام یک host است.
- Dots : نقطه ها که باعث جداسازی بخش های متفاوت خواهد شد.

هر lable توسط نقطه از یکدیگر جدا خواهند شد. هر lable می تواند حداکثر دارای ۶۳ بایت باشد. دقت داشته باشید که طول (اندازه) هر lable بر حسب بایت مشخص شده است نه بر حسب طول رشته. علت این است که DNS در ویندوز ۲۰۰۰ از کاراکترهای UTF-8 استفاده می نماید. بر خلاف کاراکترهای اسکی که قبلا" از آنان استفاده می گردید. بهرحال FQDN می بایست دارای طولی به اندازه حداکثر ۲۵۵ بایت باشد.

طراحی نام حوزه برای یک سازمان

قبل از پیاده سازی سیستم (مدل) DNS برای یک سازمان، می بایست به نمونه سوالات ذیل بدرستی پاسخ داد:

- آیا سازمان مربوطه در حال حاضر برای ارتباط اینترانتی خود از DNS استفاده می نماید؟
- آیا سازمان مربوطه دارای یک سایت اینترنتی است؟
- آیا سازمان مربوطه دارای یک حوزه(دامنه) ثبت شده (ریجستر شده) است؟
- آیا سازمان مربوطه از اسامی حوزه یکسان برای منابع مربوطه موجود بر روی
- اینترنت / اینترانت استفاده می نماید؟

استفاده از نام یکسان دامنه برای منابع اینترنت و اینترانت

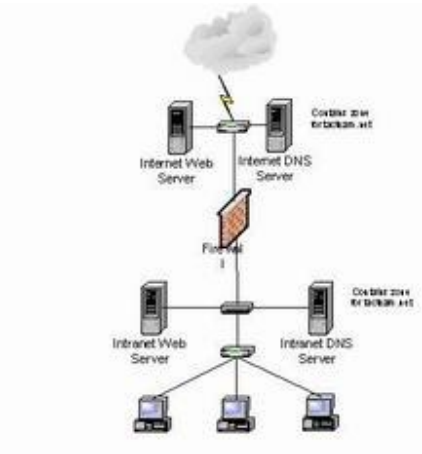
استفاده از اسامی یکسان برای نامگذاری دامنه به منظور استفاده از منابع موجود داخلی و منابع اینترنتی در مرحله اول بسیار قابل توجه و جذاب خواهد بود. تمامی

ماشین ها بعنوان عضو یک دامنه یکسان محسوب و کاربران نیاز به بخاطر سپردن دامنه های متفاوت بر اساس نوع منبع که ممکن است داخلی و یا خارجی باشد نخواهند داشت ..با توجه به وجود مزایای فوق، بکارگیری این روش می تواند باعث بروز برخی مشکلات نیز گردد. به منظور حفاظت از ناحیه (Zone) های DNS از دستیابی غیر مجاز نمی بایست هیچگونه اطلاعاتی در رابطه با منابع داخلی بر روی سرویس دهنده DNS نگهداری نمود. بنابراین می بایست برای یک دامنه از دو Zone متفاوت استفاده نمود. یکی از Zone ها منابع داخلی را دنبال و Zone دیگر مسئولیت پاسخگوئی به منابعی است که بر روی اینترنت قرار دارند. عملیات فوق قطعا" حجم وظایف مدیریت سایت را
افزایش خواهد داد.

پیاده سازی نام یکسان برای منابع داخلی و خارجی

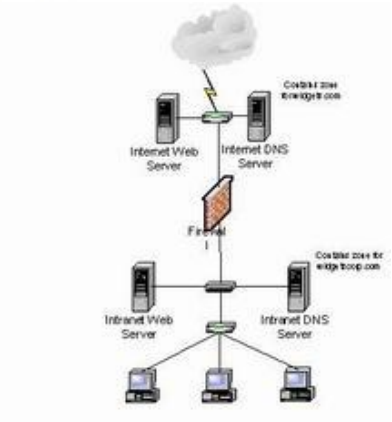
یکی دیگر از عملیاتی که می بایست در زمان پیاده سازی دامنه های یکسان برای منابع داخلی و خارجی مورد توجه قرار دارد Mirror نمودن منابع خارجی بصورت داخلی است. مثلا" فرض نمائید که Test.com نام انتخاب شده برای دستیابی به منابع داخلی (اینترانت) و منابع خارجی (اینترنت) است.درچنین وضعیتی دارای سرویس دهنده وب برا یاینترانت باشیم که پرسنل سازمان از آن به منظور دستیابی به اطلاعات اختصاصی و سایر اطلاعات داخلی سازمان استفاده می نمایند. در این مدل دارای سرویس دهندگانی خواهیم بود که به منظور دستیابی به منابع اینترنت مورد استفاده قرار خواهند گرفت. ما می خواهیم از اسامی یکسان برای سرویس دهندگان استفاده نمائیم. در مدل فوق اگر درخواستی برای www.test.com صورت پذیرد مسئله به کامپیوتری ختم خواهد شد که قصد داریم برای کاربران اینترنت قابل دستیابی باشد. در چنین وضعیتی ما نمی خواهیم کاربران اینترنت قادر به دستیابی به اطلاعات شخصی و داخلی سازمان باشند.

جهت حل مشکل فوق Mirror نمودن منابع اینترنت بصورت داخلی است و ایجاد یک zone در DNS برای دستیابی کاربران به منابع داخلی ضروری خواهد بود. زمانیکه کاربری درخواست www.test.com را صادر نمائید در ابتدا مسئله نام از طریق سرویس دهنده داخلی DNS برطرف خواهد شد که شامل zone داخلی مربوطه است. زمانی که یک کاربر اینترنت قصد دستیابی به www.test.com را داشته باشد درخواست وی به سرویس دهنده اینترنت DNS ارسال خواهدشد که در چنین حالتی آدرس IP سرویس دهنده خارجی DNS برگردانده خواهد شد.



استفاده از اسامی متفاوت برای دامنه ها ی اینترنت و اینترانت

در صورتی که سازمانی به اینترنت متصل و یا در حال برنامه ریزی جهت اتصال به اینترنت است می توان از دو نام متفاوت برای دستیابی به منابع اینترانتی و اینترنتی استفاده نمود. پیاده سازی مدل فوق بمراتب از مدل قبل ساده تر است. در مدل فوق نیازی به نگهداری Zone های متفاوت برای هر یک از آنها نبوده و هریک از آنها دارای یک نام مجزا و اختصاصی مربوط به خود خواهند بود. مثلا" می توان نام اینترنتی حوزه را Test.com و نام اینترانتی آن را TestCorp.com قرار داد.



برای نامگذاری هر یک از زیر دامنه ها می توان اسامی انتخابی را براساس نوع فعالیت و یا حوزه جغرافیائی انتخاب نمود.

Zones of Authority

DNS دارای ساختاری است که از آن برای گروه بندی و دنبال نمودن ماشین مربوطه براساس نام host در شبکه استفاده خواهد شد. به منظور فعال نمودن DNS در جهت تامین خواسته ای مورد نظر می بایست روشی جهت ذخیره نمودن اطلاعات در DNS وجود داشته باشد.اطلاعات واقعی در رابطه با دامنه ها در فایلی با نام Zone database ذخیره می گردد. این نوع فایل ها، فایل های فیزیکی بوده که بر روی سرویس دهنده DNS ذخیره خواهند شد. آدرس محل قرار گیری فایل های فوق systemroot%\system32\dns/. خواهد بود. در این بخش هدف بررسی Zone های استاندارد بوده که به دو نوع عمده تقسیم خواهند شد.

- Forward Lookup Zone
- Reverse Lookup Zone

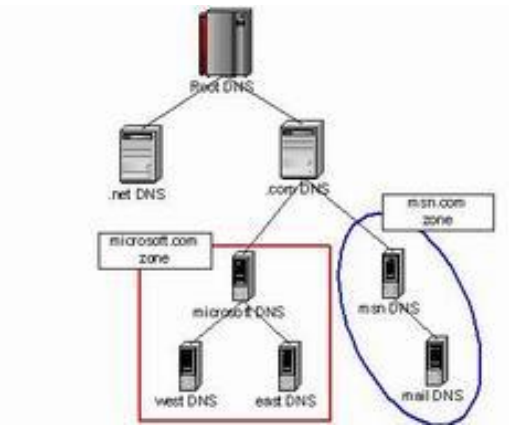
در ادامه به تشریح عملکرد هر یک از Zone های فوق خواهیم پرداخت.

Forward Lookup Zone

از این نوع Zone برای ایجاد مکانیزمی برای ترجمه اسامی host به آدرس IP برای سرویس گیرندگان DNS استفاده می گردد. Zone ها دارای اطلاعاتی هستند که بصورت رکوردهای خاص در بانک اطلاعاتی مربوطه ذخیره خواهند شد. این نوع رکوردها را " رکوردهای منبع Record Resource " می گویند. رکوردهای فوق اطلاعات مورد نیاز در رابطه با منابع قابل دسترس در هر Zone را مشخص خواهند کرد.

تفاوت بین Domain و Zone

در ابتدا می بایست به این نکته اشاره نمود که Zone ها با دامنه ها (Domain) یکسان نبوده و یک Zone می تواند شامل رکوردهائی در رابطه با چندین دامنه باشد. مثلا" فرض کنید ، دامنه www.microsoft.com دارای دو زیر دامنه با نام East , West باشد. (East.microsoft.com , West.microsoft.com). مایکروسافت دارای دامنه اختصاصی msn.com بوده که خود شامل دارای یک زیردامنه با نام mail.microsoft.com است

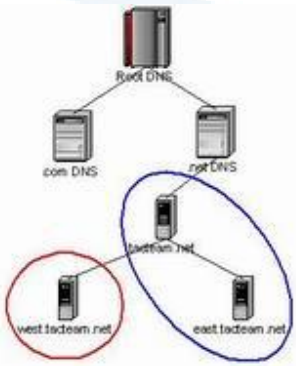


دامنه های همجوار و غیر همجوار در شکل فوق نشان داده شده است. دامنه های همجوار همدیگر را حس خواهند کرد (برای یکدیگر ملموس خواهند بود).

در رابطه با مثال فوق دامنه های موجود در Zone Microsoft.com همجوار و دامنه های Msn.com و Microsoft.com غیر همجوار هستند.

Zone ها مجوز واگذاری مسئولیت برای پشتیبانی منابع موجود در Zone را فراهم خواهند کرد. Zone ها روشی را به منظور واگذاری مسئولیت پشتیبانی و نگهداری بانک اطلاعاتی مربوطه فراهم خواهند کرد. فرض کنید شرکتی با نام TACteam وجودداشته باشد. شرکت فوق از دامنه ای با نام tacteam.net استفاده می نماید. شرکت فوق دارای شعباتی در San Francisco, Dallas، and Boston است. شعبه اصلی در Dallas بوده که مدیران متعددی برای مدیریت شبکه در آن فعالیت می نمایند. شعبه San Francisco نیز دارای چندین مدیر ورزیده به منظور نظارت بر سایت است . شعبه Boston دارای مدیریتی کارآمد برای مدیریت DNS نمی باشد. بنابراین همواره نگرانی های مربوط به واگذاری مسئولیت نگهداری بانک اطلاعاتی به یک فرد در Boston خواهیم بود. منابع موجود بر روی سایت Dallas در حوزه tacteam.net بوده و منابع موجود در San Francisco در سایت west.tacteam.net و منابع موجود در Boston در سایت east.tacteam.net نگهداری می گردنند. در چنین وضعیتی ما صرفا" دو Zone را برای مدیریت سه دامنه ایجاد خواهیم کرد. یک Zone برای tacteam.net که مسئولیت منابع مربوط به tacteam.net و east.tacteam.net را برعهده داشته و یک Zone دیگر برای west.tacteam.net که منابع موجود بر روی سایت San Francisco را برعهده خواهد گرفت . اسامی مورد نظر برای هر Zone به چه صورت می بایست انتخاب گردنند؟ هر Zone نام خود را از طریق ریشه و یا بالاترین سطح دامنه اقتباس خواهند شد. زمانیکه درخواستی برای یک منبع موجود بر روی دامنه west.tacteam.net برای DNS واصل گردد (سرویس دهنده DNS مربوط به

tacteam.net) سرویس دهنده tacteam.net صرفا" شامل یک Zone نخواهد بود.در چنین وضعیتی سرویس دهنده فوق دارای یک Delegation (واگذاری مسئولیت) بوده که به سرویس دهنده DNS مربوط به west.tacteam.net اشاره خواهد کرد. بنابراین درخواست مربوطه برای ترجمه اسامی به آدرس بدرستی به سرویس دهنده مربوطه هدایت تا مشکل برطرف گردد.



Reverse Lookup Zones

Zoneها ی از نوع Forward امکان ترجمه نام یک کامپیوتر به یک IP را فراهم می نمایند..یک Reverse Lookup این امکان را به سرویس گیرندگان خواهد داد که عملیات مخالف عملیات گفته شده را انجام دهند: ترجمه یک آدرس IP به یک نام. مثلا" فرض کنید شما می دانید که آدرس IP مربوط به کامپیوتر مقصد ۱۹۲،۱۶۸،۱،۳ است اما علاقه مند هستیم که نام آن را نیز داشته باشیم . به منظور پاسخگوئی به این نوع درخواست ها سیستم DNS از این نوع Zone ها استفاده می نماید. Zone های فوق بسادگی و راحتی Forward Zone ها رفتار نمی نمایند. مثلا" فرض کنید Forward Lookup Zone مشابه یک دفترچه تلفن باشد ایندکس این نوع دفترچه ها بر اساس نام اشخاص است .

در صورتی که قصد یافتن یک شماره تلفن را داشته باشید با حرکت بر روی حرف مربوطه و دنبال نمودن لیست که بترتیب حروف الفباء است قادر به یافتن نام شخص مورد نظر خواهید بود. اگر ما شماره تلفن فردی را بدانیم و قصد داشته باشیم از نام وی نیز آگاهی پیدا نمائیم چه نوع فرآیندی را می بایست دنبال نمود؟. از آنجائیکه دفترچه تلفن بر اساس نام ایندکس شده است تنها راه حرکت و جستجو در تمام شماره تلفن ها و یافتن نام مربوطه است .قطعا" روش فوق روش مناسبی نخواهد بود. به منظور حل مشکل فوق در رابطه با یافتن نام در صورتی که IP را داشته باشیم از یک دامنه جدید با نام in-addr.arpa استفاده می گردد. دامنه فوق اسامی مربوطه به دامنه ها را بر اساس شناسه شبکه (Network ID) ایندکس و باعث افزایش سرعت و کارآئی در بازیابی اطلاعات مورد نظر با توجه به نوع درخواست ها
خواهد شد.

با استفاده از برنامه مدیریتی DNS می توان براحتی اقدام به ایجاد این نوع Zone ها نمود. مثلا" اگر کامپیوتری دارای آدرس ۱۹۲،۱۶۸،۱،۰ باشد یک آدرس معکوس ایجاد و Zone مربوطه بصورت زیر خواهد بود :

1.168.192.in-addr.arpa.dns

نحوه عملکرد DNS

DNS ازکلمات Domain Name System اقتباس و یک پروتکل شناخته شده در عرصه شبکه های کامپیوتری خصوصا" اینترنت است. از پروتکل فوق به منظور ترجمه اسامی کامپیوترهای میزبان و Domain به آدرس های IP استفاده می گردد. زمانی که شما آدرس www.irib.ir را در مرورگر خود تایپ می نمائید، نام فوق به یک آدرس IP و بر اساس یک درخواست خاص (query) که از جانب کامپیوتر شما صادر می شود، ترجمه می گردد.

تاریخچه DNS

DNS ، زمانی که اینترنت تا به این اندازه گسترش پیدا نکرده بود و صرفا" در حد و اندازه یک شبکه کوچک بود، استفاده می گردید. در آن زمان، اسامی کامپیوترهای میزبان به صورت دستی در فایلی با نام HOSTS درج می گردید. فایل فوق بر روی یک سرویس دهنده مرکزی قرار می گرفت. هر سایت و یا کامپیوتر که نیازمند ترجمه اسامی کامپیوترهای میزبان بود، می بایست از فایل فوق استفاده می نمود. همزمان با گسترش اینترنت و افزایش تعداد کامپیوترهای میزبان، حجم فایل فوق نیز افزایش و امکان استفاده از آن با مشکل مواجه گردید (افزایش ترافیک شبکه). با توجه به مسائل فوق، در سال ۱۹۸۴ تکنولوژی DNS معرفی گردید.

پروتکل DNS

DNS ، یک "بانک اطلاعاتی توزیع شده " است که بر روی ماشین های متعددی مستقر می شود (مشابه ریشه های یک درخت که از ریشه اصلی انشعاب می شوند). امروزه اکثر شرکت ها و موسسات دارای یک سرویس دهنده DNS کوچک در سازمان خود می باشند تا این اطمینان ایجاد گردد که کامپیوترها بدون بروز هیچگونه مشکلی، یکدیگر را پیدا می نمایند. در صورتی که از ویندوز ۲۰۰۰ و اکتیو دایرکتوری استفاده می نمائید،

قطعا" از DNS به منظور ترجمه اسامی کامپیوترها به آدرس های IP ، استفاده می شود. شرکت مایکروسافت در ابتدا نسخه اختصاصی سرویس دهنده DNS خود را با نام WINS (Windows Internet Name Service) طراحی و پیاده سازی نمود. سرویس دهنده فوق مبتنی بر تکنولوژی های قدیمی بود و از پروتکل هائی استفاده می گردید که هرگز دارای کارائی مشابه DNS نبودند. بنابراین طبیعی بود که شرکت مایکروسافت از WINS فاصله گرفته و به سمت DNS حرکت کند.

از پروتکل DNS در مواردی که کامپیوتر شما اقدام به ارسال یک درخواست مبتنی بر DNS برای یک سرویس دهنده نام به منظور یافتن آدرس Domain می نماید، استفاده می شود .مثلا" در صورتی که در مرورگر خود آدرس www. Cisco.com را تایپ نمائید، یک درخواست مبتنی بر DNS از کامپیوتر شما و به مقصد یک سرویس دهنده DNS صادر می شود. ماموریت درخواست ارسالی، یافتن آدرس IP وب سایت Cisco است.

پروتکل DNS و مدل مرجع OSI

پروتکل DNS معمولا" از پروتکل UDP به منظور حمل داده استفاده می نماید. پروتکل UDP نسبت به TCP دارای overhead کمتری می باشد. هر اندازه overhead یک پروتکل کمتر باشد، سرعت آن بیشتر خواهد بود. در مواردی که حمل داده با استفاده از پروتکل UDP با مشکل و یا بهتر بگوئیم خطاء مواجه گردد، پروتکل DNS از پروتکل TCP به منظور حمل داده استفاده نموده تا این اطمینان ایجاد گردد که داده بدرستی و بدون بروز خطاء به مقصد خواهد رسید.

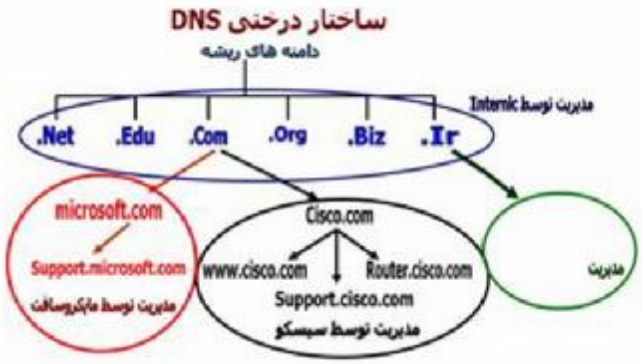
فرآیند ارسال یک درخواست DNS و دریافت پاسخ آن ، متناسب با نوع سیستم عامل نصب شده بر روی یک کامپیوتر است .برخی از سیستم های عامل اجازه استفاده از پروتکل TCP برای DNS را نداده و صرفا" می بایست از پروتکل UDP به منظور حمل داده استفاده شود . بدیهی است در چنین مواردی همواره این احتمال وجود خواهد داشت که با خطاهائی مواجه شده و عملا" امکان ترجمه نام یک کامپیوتر و یا Domain به آدرس IP وجود نداشته باشد.

پروتکل DNS از پورت ۵۳ به منظور ارائه خدمات خود استفاده می نماید. بنابراین یک سرویس دهنده DNS به پورت ۵۳ گوش داده و این انتظار را خواهد داشت که هر سرویس گیرنده ای که تمایل به استفاده از سرویس فوق را دارد از پورت مشابه استفاده نماید. در برخی موارد ممکن است مجبور شویم از پورت دیگری استفاده نمائیم. وضعیت فوق به سیستم عامل و سرویس دهنده DNS نصب شده بر روی یک کامپیوتر بستگی دارد.

ساختار سرویس دهندگان نام دامنه ها در اینترنت

امروزه بر روی اینترنت میلیون ها سایت با اسامی Domain ثبت شده وجود دارد. شاید این سوال برای شما تاکنون مطرح شده باشد که این اسامی چگونه سازماندهی می شوند؟ ساختار DNS بگونه ای طراحی شده است که یک سرویس دهنده DNS ضرورتی به آگاهی از تمامی اسامی Domain ریجستر شده نداشته و صرفا" میزان آگاهی

وی به یک سطح بالاتر و یک سطح پائین تر از خود محدود می گردد . شکل زیر بخش های متفاوت ساختار سلسله مراتبی DNS را نشان می دهد:



internic ، مسئولیت کنترل دامنه های ریشه را برعهده داشته که شامل تمامی Domain های سطح بالا می باشد (در شکل فوق به رنگ آبی نشان داده شده است). در بخش فوق تمامی سرویس دهندگان DNS ریشه قرار داشته و آنان دارای آگاهی لازم در خصوص دامنه های موجود در سطح پائین تر از خود می باشند (مثلا" microsoft.com). سرویس دهندگان DNS ریشه مشخص خواهند کرد که کدام سرویس دهنده DNS در ارتباط با دامنه های microsoft.com و یا Cisco.com می باشد.

هر domain شامل یک Primary DNS و یک Secondary DNS می باشد. Primary DNS ، تمامی اطلاعات مرتبط با Domain خود را نگهداری می نماید. Secondary DNS به منزله یک backup بوده و در مواردی که Primary DNS با مشکل مواجه می شود از آن استفاده می گردد. به فرآیندی که بر اساس آن یک سرویس دهنده Primary DNS اطلاعات خود را در سرویس دهنده Secondary DNS تکثیر می نماید ، Zone Transfer گفته می شود.

امروزه صدها وب سایت وجود دارد که می توان با استفاده از آنان یک Domain را ثبت و یا اصطلاحا" ریجستر نمود . پس از ثبت یک Domain ، امکان مدیریت آن در اختیار شما گذاشته شده و می توان رکوردهای منبع (RR) را در آن تعریف نمود.

Support, www و Routers ، نمونه هائی از رکوردهای منبع در ارتباط با دامنه Cisco.com می باشد. به منظور ایجاد Subdomain می توان از یک برنامه مدیریتی DNS استفاده نمود. www و یا هر نوع رکورد منبع دیگری را می توان با استفاده از اینترفیس فوق تعریف نمود . پس از اعمال تغییرات دلخواه خود در ارتباط با Domain ، محتویات فایل های خاصی که بر روی سرویس دهنده ذخیره شده اند نیز تغییر نموده و در ادامه تغییرات فوق به سایر سرویس دهندگان تائید شده اطلاع داده می شود. سرویس دهندگان فوق، مسئولیت Domain شما را برعهده داشته و در ادامه تمامی اینترنت که به این سرویس دهندگان DNS متصل می شوند از تغییرات ایجاد شده آگاه و قادر به برقراری ارتباط با هر یک از بخش های Domain می گردند. مثلا" در صورتی که قصد ارتباط با Support.Cisco.com را داشته باشید، کامپیوتر شما با سرویس دهنده DNS که مسئولیت مدیریت دامنه های Com. را دارد، ارتباط برقرار نموده و سرویس دهنده فوق اطلاعات لازم در خصوص دامنه Cisco.com را در اختیار قرار خواهد داد . در نهایت سرویس دهنده DNS مربوط به Cisco.com (سرویس دهنده فوق، تمامی اطلاعات مرتبط با دامنه Cisco.com را در خود نگهداری می نماید)، آدرس IP کامپیوتر مربوط به Support.Cisco.com را مشخص نموده تا امکان برقراری ارتباط با آن فراهم گردد.

نحوه ترجمه اسامی Domain توسط DNS

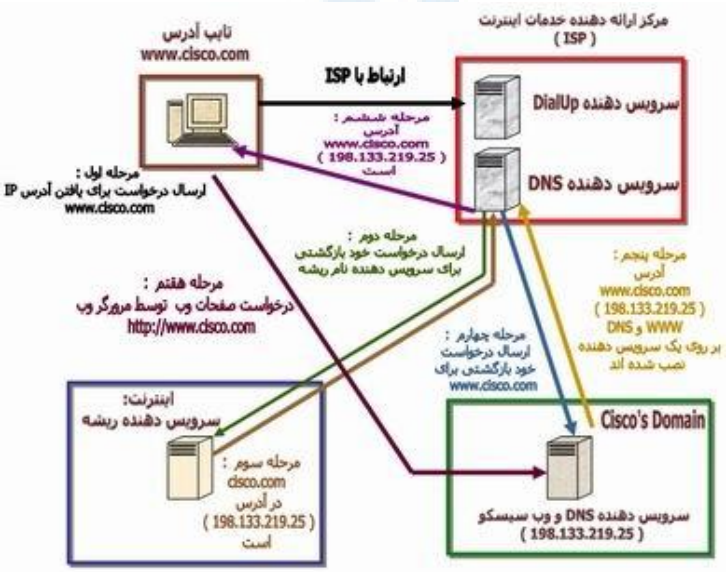
آیا تاکنون این سوال برای شما مطرح شده است که پس از تایپ نام یک سایت در مرورگر وب، آدرس IP آن چگونه پیدا می شود؟ برای ارتباط با یک سایت، می بایست قبل از هر چیز آدرس IP آن مشخص گردد . به منظور ترجمه اسامی کامپیوترهای میزبان و Domain به آدرس های IP از پروتکل DNS استفاده می گردد.

Queries و Resolution

یک سرویس گیرنده به منظور استفاده از DNS و اخذ پاسخ لازم از دو روش متفاوت استفاده می نماید:

- **در روش اول** ، سرویس گیرنده با سرویس دهندگان نام ارتباط برقرار می نماید. فرآیند فوق مادامیکه سرویس دهنده مجاز شامل اطلاعات مورد نیاز پیدا نشود، ادامه خواهد یافت (روش non Recursive query).
- **در روش دوم** ، ماموریت ترجمه نام به آدرس به DNS واگذار می شود. در این روش سرویس گیرنده اقدام به ارسال درخواست خود برای DNS نموده و DNS پس از انجام عملیاتی خاص و یافتن آدرس IP سایت درخواستی، آن را برای سرویس گیرنده ارسال می نماید (روش Recursive query).

شکل زیر نحوه انجام کار در روش دوم را نشان می دهد:



به منظور آشنائی با نحوه انجام عملیات فوق به بررسی یک نمونه مثال می پردازیم.
زمانی که شما قصد مشاهده یک وب سایت نظیروب سایت(www.cisco.com) را داشته باشید،
پس از فعال نمودن مرورگر وب و تایپ آدرس http://www.cisco.com و یا www.cisco.com ، پس از مدت زمان کوتاهی ! صفحه اصلی وب سایت در مرورگر شما نمایش داده می شود. برای یافتن آدرس IP وب سایت درخواستی مراحل زیر دنبال می شود :

- **مرحله اول** : فعال نمودن مرورگر و درج آدرس www.cisco.com در بخش آدرس آن . در این مقطع کامپیوتر شما دارای آگاهی لازم در خصوص آدرس IP وب سایت سیسکو نمی باشد. بنابراین یک درخواست DNS را برای سرویس دهنده DNS مربوط به مرکز ارائه دهنده سرویس های اینترنت (ISP) ارسال می نماید. حتما" این سوال برای شما مطرح شده است که کامپیوتر به چه صورت از آدرس IP سرویس دهنده DNS آگاهی می یابد تا درخواست خود را برای وی ارسال نماید ؟ در صورتی که شما از طریق up-Dial به اینترنت متصل شده اید ، این موضوع با استفاده از تنظیمات انجام شده (ایستا و پویا) پروتکل TCP/IP مرتبط با آداپتور مجازی up-Dial انجام خواهد شد. در صورتی که دارای یک اتصال دائم به اینترنت و از طریق یک شبکه محلی می باشید، این موضوع با استفاده ازتنظیمات انجام شده (ایستا و پویا) پروتکلTCP/IP مرتبط با آداپتور کارت شبکه انجام خواهد شد.

مرحله دوم : سرویس دهنده DNS مرکز ارائه دهنده خدمات اینترنت (ISP) شما، آدرس IP مربوط به سایت سیسکو را نمی داند و بدین دلیل، آدرس سایت فوق را از یکی از سرویس دهندگان نام ریشه درخواست می نماید.

- **مرحله سوم** : سرویس دهنده DNS ریشه، بانک اطلاعاتی خود را بررسی نموده و از سرویس دهنده DNS اولیه Cisco.com آگاهی می یابد (IP :

۱۹۸،۱۳۳،۲۱۹،۲۵) . پس از آگاهی از آدرس IP سرویس دهنده DNS مربوط به cisco.com ، پاسخ لازم برای سرویس دهنده ISP شما ارسال می گردد.

- **مرحله چهارم** : در این مرحله سرویس دهنده DNS مرکز ISP شما دانش لازم به منظور ارتباط با سرویس دهنده DNS سیسکو را پیدا نموده و پس از برقراری ارتباط از وی آدرس IP وب سایت سیسکو (www.cisco.com) را جویا می شود. بدین منظور سرویس دهنده شما یک درخواست Recursive را برای سرویس دهنده DNS مربوط به Cisco.com ارسال می نماید.
- **مرحله پنجم** : سرویس دهنده DNS سیسکو، بانک اطلاعاتی خود را بررسی نموده و از وجود رکورد www.cisco.com در بانک آگاه می گردد. رکورد فوق دارای یک آدرس IP معادل IP:198.133.219.25 است. در این حالت خاص، سرویس دهنده وب بر روی ماشین مشابهی است که سرویس دهنده DNS نصب شده است. در صورتی که سرویس دهنده وب و سرویس دهنده DNS بر روی یک ماشین مشابه نصب نشده باشند، آدرس IP آنان متفاوت بوده و این موضوع از طریق رکوردهای منبع موجود در بانک اطلاعاتی سرویس دهنده DNS مشخص می گردد.
- **مرحله ششم** : سرویس دهنده DNS مربوط به ISP شما از آدرس IP مربوط به www.cisco.com آگاهی پیدا نموده و نتایج را برای کامپیوتر شما ارسال می نماید.
- **مرحله هفتم** : کامپیوتر شما در این مقطع دارای آگاهی لازم در خصوص آدرس IP وب سایت سیسکو بوده و می تواند با آن ارتباط برقرار نماید. بنابراین کامپیوتر شما یک درخواست http را مستقیماً برای سرویس دهنده وب سیسکو ارسال نموده و از وی درخواست یک صفحه وب را می نماید.

اترنت

دستیابی به اطلاعات با روش های مطمئن و با سرعت بالا یکی از رموز موفقیت هر سازمان و موسسه است. طی سالیان اخیر هزاران پرونده و کاغذ که حاوی اطلاعات با ارزش برای یک سازمان بوده ، در کامپیوتر ذخیره شده اند. با تغذیه دریائی از اطلاعات به کامپیوتر، امکان **مدیریت الکترونیکی** اطلاعات فراهم شده است. کاربران متفاوت در اقصی نقاط جهان قادربه اشتراک اطلاعات بوده وتصویری زیبا از همیاری وهمکاری اطلاعاتی را به نمایش می گذارند.

شبکه های کامپیوتری در این راستا و جهت نیل به اهداف فوق نقش بسیار مهمی را ایفاء می نمایند.اینترنت که عالی ترین تبلور یک شبکه کامپیوتری در سطح جهان است، امروزه در مقیاس بسیار گسترده ای استفاده شده و ارائه دهندگان اطلاعات، اطلاعات و یا فرآورده های اطلاعاتی خود را در قالب محصولات تولیدی و یا خدمات در اختیار استفاده کنندگان قرارمی دهند. وب که عالی ترین سرویس خدماتی اینترنت می باشد کاربران را قادر می سازد که در اقصی نقاط دنیا اقدام به خرید، آموزش، مطالعه و ... نمایند.

با استفاده از شبکه، یک کامپیوتر قادر به ارسال و دریافت اطلاعات از کامپیوتر دیگر است. اینترنت نمونه ای عینی از یک شبکه کامپیوتری است. در این شبکه میلیون ها کامپیوتر در اقصی نقاط جهان به یکدیگر متصل شده اند.اینترنت شبکه ای است مشتمل بر زنجیره ای از شبکه های کوچکتراست . نقش شبکه های کوچک برای ایجاد تصویری با نام اینترنت بسیار حائز اهمیت است. تصویری که هر کاربر با نگاه کردن به آن گمشده خود را در آن پیدا خواهد کرد. در این بخش به بررسی شبکه های کامپیوتری و جایگاه مهم آنان در زمینه تکنولوژی اطلاعات و مدیریت الکترونیکی اطلاعات خواهیم داشت.

شبکه های محلی و شبکه های گسترده

تاکنون شبکه های کامپیوتری بر اساس مولفه های متفاوتی تقسیم بندی شده اند. یکی از این مولفه ها " حوزه جغرافیائی " یک شبکه است. بر همین اساس شبکه ها به دو گروه عمده **LAN**(Local area network) و **WAN** (Wide area network) تقسیم می گردند. در شبکه های LAN مجموعه ای از دستگاه های موجود در یک حوزه جغرافیائی محدود، نظیر یک ساختمان به یکدیگر متصل می گردند. در شبکه های WAN تعدادی دستگاه که از یکدیگر کیلومترها فاصله دارند به یکدیگر متصل خواهند شد. مثلا" اگر دو کتابخانه که هر یک در یک ناحیه از شهر بزرگی مستقر می باشند، قصد اشتراک اطلاعات را داشته باشند، می بایست شبکه ای WAN ایجاد و کتابخانه ها را به یکدیگر متصل نمود. برای اتصال دو کتابخانه فوق می توان از امکانات مخابراتی متفاوتی نظیر خطوط اختصاصی (Leased) استفاده نمود. شبکه های LAN نسبت به شبکه های WAN دارای سرعت بیشتری می باشند. با رشد و توسعه دستگاههای متفاوت مخابراتی میزان سرعت شبکه های WAN، تغییر و بهبود پیدا کرده است. امروزه با بکارگیری و استفاده از فیبر نوری در شبکه های LAN امکان ارتباط دستگاههای متعدد که در مسافت های طولانی نسبت بیکدیگر قرار دارند، فراهم شده است.

اترنت

در سال ۱۹۷۳ پژوهشگری با نام " Metcalfe" در مرکز تحقیقات شرکت زیراکس، اولین شبکه اترنت را بوجود آورد. هدف وی ارتباط کامپیوتر به یک چاپگر بود. وی روشی فیزیکی به منظور کابل کشی بین دستگاههای متصل بهم در اترنت ارائه نمود. اترنت در مدت زمان کوتاهی به عنوان یکی از تکنولوژی های رایج برای برپاسازی شبکه در سطح دنیا مطرح گردید. همزمان با پیشرفت های مهم در زمینه شبکه های کامپیوتری ، تجهیزات و دستگاه های مربوطه، شبکه های اترنت نیز همگام با تحولات فوق شده و قابلیت های متفاوتی را در بطن خود ایجاد نمود. با توجه به

تغییرات و اصلاحات انجام شده در شبکه های اترنت ،عملکرد و نحوه کار آنان نسبت به شبکه های اولیه تفاوت چندانی نکرده است . در اترنت اولیه، ارتباط تمام دستگاه های موجود در شبکه از طریق یک کابل انجام می گرفت که توسط تمام دستگاهها به اشتراک گذاشته می گردید. پس از اتصال یک دستگاه به کابل مشترک، می بایست پتانسیل های لازم به منظور ایجاد ارتباط با سایر دستگاههای مربوطه نیز در بطن دستگاه وجود داشته باشد (کارت شبکه). بدین ترتیب امکان گسترش شبکه به منظور استفاده از دستگاههای جدید براحتی انجام و نیازی به اعمال تغییرات بر روی دستگاههای موجود در شبکه نخواهد بود.

اترنت یک تکنولوژی محلی (**LAN**) است. اکثر شبکه های اولیه در حد و اندازه یک ساختمان بوده و دستگاهها نزدیک به هم بودند. دستگاههای موجود بر روی یک شبکه اترنت صرفا" قادر به استفاده از چند صد متر کابل بیشترنبودند.اخیرا" با توجه به توسعه امکانات مخابراتی و محیط انتقال، زمینه استقرار دستگاههای موجود در یک شبکه اترنت با مسافت های چند کیلومترنیز فراهم شده است.

پروتکل

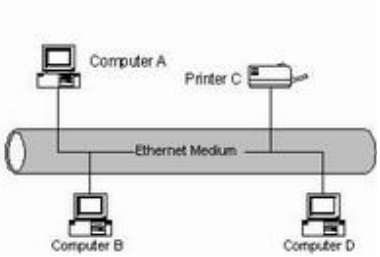
پروتکل در شبکه های کامپیوتری به مجموعه قوانینی اطلاق می گردد که نحوه ارتباطات را قانونمند می نماید. نقش پروتکل در کامپیوتر نظیر نقش زبان برای انسان است. برای مطالعه یک کتاب نوشته شده به فارسی می بایست خواننده شناخت مناسبی از زبان فارسی را داشته باشد. به منظور ارتباط موفقیت آمیز دو دستگاه در شبکه می بایست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

اصطلاحات اترنت

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

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

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



یک سیگنال اترنت بر روی محیط انتقال به هر یک از گره های متصل شده در محیط انتقال خواهد رسید. بنابراین مشخص شدن آدرس مقصد، به منظوردریافت پیام نقشی

حیاتی دارد. مثلا" در صورتی که کامپیوتر B (شکل بالا) اطلاعاتی را برای چاپگر C ارسال می دارد کامپیوترهای A و D نیز فریم را دریافت و آن را بررسی خواهند کرد. هر ایستگاه زمانیکه فریم را دریافت می دارد، آدرس آن را بررسی تا مطمئن گردد که پیام برای وی ارسال شده است یا خیر؟ در صورتی که پیام برای ایستگاه مورد نظر ارسال نشده باشد، ایستگاه فریم را بدون بررسی محتویات آن کنارخواهدگـــذاشت(عدم استفاده).

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

CSMA/CD

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

به منظور شناخت تکنولوژی فوق مثال زیر را دنبال می نمائیم.

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

باشد می بایست گوش خود را بر روی محیط انتقال گذاشته و بررسی نماید که آیا محیط انتقال آزاد است؟ در صورتی که صدائی از محیط انتقال به گوش ایستگاه متقاضی ارسال اطلاعات نرسد، ایستگاه مورد نظر قادر به استفاده از محیط انتقال و ارسال اطلاعات خواهد بود.

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

محدودیت های اترنت

یک شبکه اترنت دارای محدودیت های متفاوت از ابعاد گوناگون (بکارگیری تجهیزات) است. طول کابلی که تمام ایستگاهها بصورت اشتراکی از آن به عنوان محیط انتقال استفاده می نمایند یکی از شاخص ترین موارد در این زمنیه است. سیگنال های الکتریکی در طول کابل بسرعت منتشر می گردند. همزمان با طی مسافتی، سیگنال ها ضعیف می گردند. وجود میدان های الکتریکی که توسط دستگاههای مجاور کابل نظیرلامپ های فلورسنت ایجاد می گردد، باعث تلف شدن سیگنال می گردد. طول کابل شبکه می بایست کوتاه بوده تا امکان دریافت سیگنال توسط دستگاه های موجود در دو نقطه ابتدائی و انتهائی کابل بصورت شفاف و با حداقل تاخیر زمانی فراهم گردد. همین امر باعث بروز محدودیت در طول کابل استفاده شده، می گردد. پروتکل CSMA/CD امکان ارسال اطلاعات برای صرفا" یک دستگاه را در هر لحظه فراهم می نماید، بنابراین محدودیت هائی از لحاظ تعداد دستگاههائی که می توانند بر روی یک شبکه مجزا وجود داشته باشند، نیز بوجود خواهد آمد. با اتصال دستگاه های متعدد (فراوان) بر روی یک سگمنت مشترک، شانس استفاده از محیط انتقال برای هر یک از دستگاه های موجود بر روی سگمنت کاهش پیدا خواهد کرد. در این حالت هر دستگاه به منظور ارسال اطلاعات می بایست مدت زمان زیادی را در انتظار سپری نماید. تولید کنندگان تجهیزات شبکه دستگاه های متفاوتی را به منظور غلبه بر مشکلات و محدودیت گفته شده، طراحی و عرضه نموده اند. اغلب دستگاههای فوق مختص شبکه های اترنت نبوده ولی در سایر تکنولوژی های مرتبط با شبکه نقش مهمی را ایفاء می نمایند.

تکرارکننده (Repeater)

اولین محیط انتقال استفاده شده در شبکه های اترنت کابل های مسی کواکسیال بود که Thicknet (ضخیم) نامیده می شوند. حداکثر طول یک کابل ضخیم ۵۰۰ متر است . در یک ساختمان بزرگ ، کابل ۵۰۰ متری جوابگوی تمامی دستگاه های شبکه نخواهد

بود. تکرار کننده ها با هدف حل مشکل فوق، ارائه شده اند. . تکرارکننده ها ، سگمنت های متفاوت یک شبکه اترنت را به یکدیگر متصل می کنند. در این حالت تکرارکننده سیگنال ورودی خود را از یک سگمنت اخذ و با تقویت سیگنال آن را برای سگمنت بعدی ارسال خواهد کرد. بدین تزتیب با استفاده از چندین تکرار کننده و اتصال کابل های مربوطه توسط آنان، می توان قطر یک شبکه را افزایش داد. (قطر شبکه به حداکثر مسافت موجود بین دو دستگاه متمایز در شبکه اطلاق می گردد)

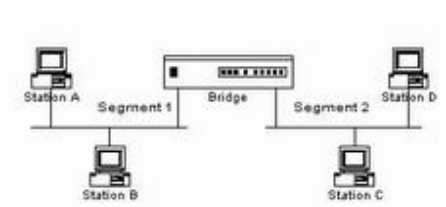
Bridges و سگمنت

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

به منظور حل مشکل فوق، Bridges در شبکه اترنت پیاده سازی شده است . Bridge دو و یا چندین سگمنت را به یکدیگر متصل خواهد کرد. بدین ترتیب دستگاه فوق باعث افزایش قطر شبکه خواهد شد. عملکرد Bridge از بعد افزایش قطر شبکه نظیر تکرارکننده است، با این نفاوت که Bridge قادر به ایجاد نظم در ترافیک شبکه نیز خواهد بود. Bridge نظیر سایر دستگاههای موجود در شبکه قادر به ارسال و دریافت اطلاعات بوده ولی عملکرد آنها دقیقا" مشابه یک ایستگاه نمی باشد. Bridge قادر به

ایجاد ترافیکی که خود سرچشمه آن خواهد بود، نیست (نظیر تکرارکننده) .Bridge صرفا" چیزی را که از سایر ایستگاهها می شنود، منعکس می نماید. (Bridge قادر به ایجا د یک نوع فـــریم خاص اترنت به منظور ایـــجاد ارتبـاط با ســـایر Bridge ها می باشند).

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



همانگونه که در شکل فوق مشاهده می گردد Bridge دو سگمنت را به یکدیگر متصل نموده است . در صورتی که ایستگاه A و یا B قصد ارسال اطلاعات را داشته باشند Bridge نیز فریم های اطلاعاتی را دریافت خواهد کرد. نحوه برخورد Bridge با فریم های اطلاعاتی دریافت شده به چه صورت است؟ آیا قادر به ارسال اتوماتیک فریم ها برای سگمنت دوم می باشد؟ یکی ازاهداف استفاده از Bridge کاهش ترافیک های غیرضروری در هر سگمنت است. در این راستا، آدرس مقصد فریم ، قبل از هر گونه عملیات بر روی آن، بررسی خواهد شد. در صورتی که آدرس مقصد، ایستگاههای A و یا B باشد نیازی به ارسال فریم برای سگمنت شماره دو وجود نخواهد داشت. در این حالت Bridge عملیات خاصی را انجام نخواهد داد. نحوه برخورد Bridge با فریم فوق مشابه فیلتر نمودن است. درصورتی که آدرس مقصد فریم یکی از ایستگاههای C و یا D باشد و یا فریم مورد نظر دارای یک آدرس از نوع Broadcast باشد، Bridge فریم فوق را برای سگمنت شماره دو ارسال خواهد کرد.

با ارسال و هدایت فریم اطلاعاتی توسط Bridge امکان ارتباط چهار دستگاه موجود در شبکه فراهم می گردد. با توجه به مکانیزم فیلتر نمودن فریم ها توسط Bridge ، این امکان بوجود خواهد آمد که ایستگاه A اطلاعاتی را برای ایستگاه B ارسال و در همان لحظه نیز ایستگاه C اطلاعاتی را برای ایستگاه D ارسال نماید.بدین ترتیب امکان برقراری دو ارتباط بصورت همزمان بوجود آمده است.

روترها : سگمنت های منطقی

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

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

وضعیت فعلی اترنت

از زمان مطرح شدن شبکه های اترنت تاکنون تغییرات فراوانی از بعد تنوع دستگاه های مربوطه ایجاد شده است . در ابتدا از کابل کواکسیال در این نوع شبکه ها استفاده می گردید.امروزه شبکه های مدرن اترنت از کابل های بهم تابیده و یا فیبر نوری برای اتصال ایستگاه ها به یکدیگر استفاده می نمایند. در شبکه های اولیه اترنت سرعت انتقال اطلاعات ده مگابیت در ثانیه بود ولی امروزه این سرعت به مرز ۱۰۰و حتی ۱۰۰۰ مگابیت در ثانیه رسیده است. مهمترین تحول ایجاد شده در شبکه های اترنت امکان استفاده از سوئیچ های اترنت است .سگمنت ها توسط سوئیچ به یکدیگر متصل می گردند. (نظیر Bridge با این تفاوت عمده که امکان اتصال چندین سگمنت توسط سوئیچ فراهم می گردد) برخی از سوئیچ ها امکان اتصال صدها سگمنت به یکدیگر را فراهم می نمایند. تمام دستگاههای موجود در شبکه، سوئیچ و یا ایستگاه می باشند . قبل از ارسال فریم های اطلاعاتی برا ی هر ایستگاه، سوئیچ فریم مورد نظر را دریافت و پس از بررسی، آن را برای ایستگاه مقصد مورد نظر ارسال خواهد کرد. عملیات فوق مشابه Bridge است، ولی در مدل فوق هر سگمنت دارای صرفا" یک ایستگاه است و فریم صرفا" به دریافت کننده واقعی ارسال خواهد شد. بدین ترتیب امکان برقراری ارتباط همزمان بین تعداد زیادی ایستگاه در شبکه های مبتنی بر سوئـــیچ فراهم خواهد شد.

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

بوده و همزمان با ارسال اطلاعات توسط یک ایستگاه به سوئیچ ، امکان ارسال اطلاعات توسط سوئیچ برای ایستگاه دیگر نیز فراهم خواهد شد.

اترنت و استاندارد ۸۰۲،۳

شاید تاکنون اصطلاح ۸۰۲،۳ را در ارتباط با شبکه های اترنت شنیده باشید. اترنت به عنوان یک استاندارد شبکه توسط شرکت های: دیجیتال، اینتل و زیراکس (DIX) مطرح گردید. در سال ۱۹۸۰ موسسه IEEE کمیته ای را مسئول استاندار سازی تکنولوژی های مرتبط با شبکه کرد. موسسه IEEE نام گروه فوق را ۸۰۲ قرار داد. (عدد ۸۰۲ نشاندهنده سال و ماه تشکیل کمیته استانداردسازی است) کمیته فوق از چندین کمیته جانبی دیگر تشکیل شده بود. هر یک از کمیته های فرعی نیز مسئول بررسی جنبه های خاصی از شبکه گردیدند. موسسه IEEE برای تمایز هر یک از کمیته های جانبی از روش نامگذاری: X،۸۰۲ استفاده کرد. X یک عدد منصر بفرد بوده که برای هر یک از کمیته ها در نظر گرفته شده بود . گروه ۸۰۲،۳ مسئولیت استاندارد سازی عملیات در شبکه های CSMA/CD را برعهده داشتند. (شبکه فوق در ابتدا DIX Ethernet نامیده می شد) اترنت و ۸۰۲،۳ از نظر فرمت داده ها در فریم های اطلاعاتی با یکدیگر متفاوت می باشند.

تکنولوژی های متفاوت شبکه

متداولترین مدل موجود در شبکه های کامپیوتری (رویکرد دیگری از اترنت) توسط شرکت IBM و با نام ring Token عرضه گردید. در شبکه های اترنت به منظور دستیابی از محیط انتقال از فواصل خالی (Gap) تصادفی در زمان انتقال فریم ها استفاده می گردد. شبکه های Token ring از یک روش پیوسته در این راستا استفاده می نمایند. در شبکه های فوق، ایستگاه ها از طریق یک حلقه منطقی به یکدیگر متصل می گردند. فریم ها صرفا" در یک جهت حرکت و پس از طی طول حلقه، فریم کنار

گذاشته خواهد شد. روش دستیابی به محیط انتقال برای ارسال اطلاعات تابع CSMA/CD نخواهد بود و از روش passing Token استفاده می گردد. در روش فوق در ابتدا یک Token (نوع خاصی از یک فریم اطلاعاتی) ایجاد می گردد. Token فوق در طول حلقه می چرخد . زمانیکه یک ایستگاه قصد ارسال اطلاعات را داشته باشد، می بایست Token را در اختیار گرفته و فریم اطلاعاتی خود را بر روی محیط انتقال ارسال دارد. زمانیکه فریم ارسال شده مجدداً" به ایستگاه ارسال کننده برگشت داده شد (طی نمودن مسیر حلقه)، ایستگاه فریم خود را حذف و یک Token جدید را ایجاد وآن را بر روی حلقه قرار خواهد داد. در اختیار گرفتن Token شرط لازم برا ی ارسال اطلاعات است. سرعت ارسال اطلاعات در این نوع شبکه ها چهار تا شانزده مگابیت در ثانیه است.

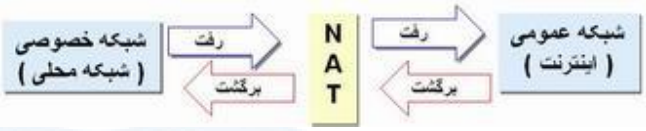
اترنت با یک روند پیوسته همچنان به رشد خود ادامه می دهد. پس از گذشت حدود سی سال ازعمر شبکه های فوق استانداردهای مربوطه ایجاد و برای عموم متخصصین شناخته شده هستند و همین امر نگهداری و پشتیبانی شبکه های اترنت را آسان نموده است. اترنت با صلابت بسمت افزایش سرعت و بهبود کارآئی و عملکرد گام برمی دارد.

NAT

اینترنت با سرعتی باورنکردنی همچنان در حال گسترش است. تعداد کامپیوترهای ارائه دهنده اطلاعات (خدمات) و کاربران اینترنت روزانه تغییر و رشد می یابد. با اینکه نمی توان دقیقا" اندازه اینترنت را مشخص کرد ولی تقریبا" یکصد میلیون کامپیوتر میزبان (Host) و ۳۵۰ میلیون کاربر از اینترنت استفاده می نمایند. رشد اینترنت چه نوع ارتباطی با Network Address Translator (**NAT**) دارد؟ هر کامپیوتر به منظور ارتباط با سایر کامپیوترها و سرویس دهندگان وب بر روی اینترنت، می بایست دارای یک آدرس IP باشد. IP یک عدد منحصر بفرد ۳۲ بیتی بوده که کامپیوتر موجود در یک شبکه را مشخص می کند.

اولین مرتبه ای که مسئله آدرس دهی توسط IP مطرح گردید، کمتر کسی به این فکر می افتاد که ممکن است خواسته ای مطرح شود که نتوان به آن یک آدرس را نسبت داد. با استفاده از سیستم آدرس دهی IP می توان ٤،٢٩٤،٩٧٦،٢٩٦ ($٢^{٣٢}$) آدرس را تولید کرد. (بصورت تئوری). تعداد واقعی آدرس های قابل استفاده کمتر از مقدار (بین ۳،۲ میلیارد و ۳،۳ میلیارد) فوق است. علت این امر، تفکیک آدرس ها به کلاس ها و رزو بودن برخی آدرس ها برای multicasting ، تست و موارد خاص دیگر است. همزمان با انفجار اینترنت (عمومیت یافتن) و افزایش شبکه های کامپیوتری، تعداد IP موجود، پاسخگوی نیازها نبود. منطقی ترین روش، طراحی مجدد سیستم آدرس دهی IP است تا امکان استفاده از آدرس های IP بیشَتری فراهم گردد. موضوع فوق در حال پیاده سازی بوده و نسخه شماره شش IP ، راهکاری در این زمینه است . چندین سال طول خواهد کشید تا سیستم فوق پیاده سازی گردد، چراکه می بایست تمامی زیرساخت های اینترنت تغییر واصلاح گردند.NAT با هدف کمک به مشکل فوق طراحی شده است. NAT به یک دستگاه اجازه می دهد که بصورت یک روتر عمل نماید. در این حالت NAT به عنوان یک آژانس بین اینترنت (شبکه عمومی) و یک شبکه محلی

(شبکه خصوصی) رفتار نماید. این بدان معنی است که صرفا" یک IP منحصر بفرد به منظور نمایش مجموعه ای از کامپیوترها(یک گروه) مورد نیاز خواهد بود.



کم بودن تعداد IP صرفا" یکی از دلایل استفاده از NAT است .در ادامه به بررسی علل استفاده از NATخواهیم پرداخت.

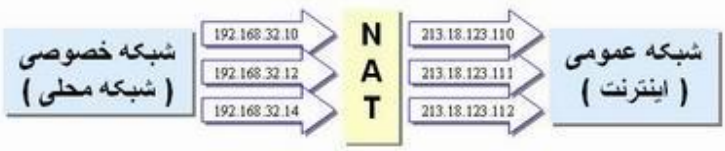
قابلیت های NAT

عملکرد NAT مشابه یک تلفتچی در یک اداره بزرگ است. فرض کنید شما به تلفنچی اداره خود اعلام نموده اید که تماس های تلفنی مربوط به شما را تا به وی اعلام ننموده اید ، وصل نکند. در ادامه با یکی ازمشتریان تماس گرفته و برای وی پیامی گذاشته اید که سریعا" با شما تماس بگیرد. شما به تلفتچی اداره می گوئید که منتظر تماس تلفن از طرف یکی از مشتریان هستم، در صورت تماس وی، آن را به دفتر من وصل نمائید. در ادامه مشتری مورد نظر با اداره شما تماس گرفته و به تلفنچی اعلام می نماید که قصد گفتگو با شما را دارد (چراکه شما منتظر تماس وی هستید). تلفنچی جدول مورد نظر خود را بررسی تا نام شما را در آن پیدا نماید. تلفنچی متوجه می شود که شما تلفن فوق را درخواست نموده اید، بنابراین تماس مورد نظر به دفتر شما وصل خواهد شد.

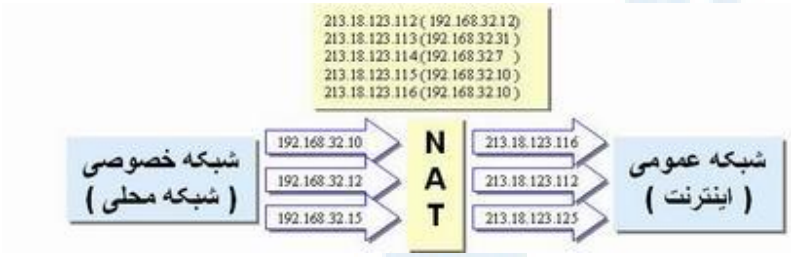
NAT توسط شرکت سیسکو و به منظور استفاده در یک دستگاه (فایروال، روتر، کامپیوتر) ارائه شده است.NAT بین یک شبکه داخلی و یک شبکه عمومی مستقر و شامل مدل ها ی متفاوتی است.

- **NAT ایستا** . عملیات مربوط به ترجمه یک آدرس IP غیر ریجستر شده (ثبت شده) به یک آدرس IP ریجستر شده را انجام می دهد. (تناظر یک به یک) روش فوق زمانیکه قصد استفاده از یک دستگاه را از طریق خارج از شبکه

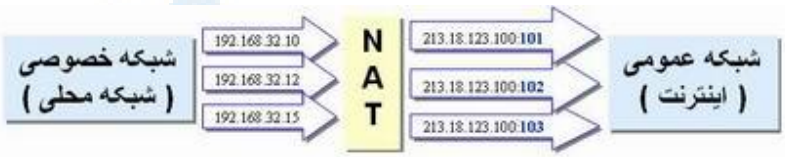
داشته باشیم، مفید و قابل استفاده است. در مدل فوق همواره IP 192.168.32.10 به IP 213.18.123.110 ترجمه خواهد شد.



- **NAT پویا** . یک آدرس IP غیر ریجستر شده را به یک IP ریجستر شده ترجمه می نماید. در ترجمه فوق از گروهی آدرس های IP ریجستر شده استفاده خواهد شد.

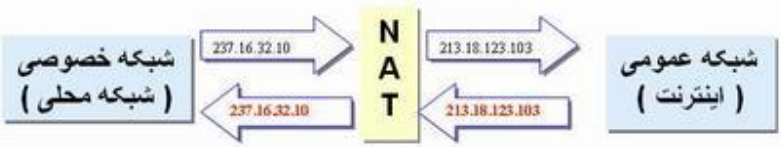


- **OverLoading** . مدل فوق شکل خاصی از NAT پویا است. در این مدل چندین IP غیر ریجستر شده به یک IP ریجستر شده با استفاده از **پورت های** متعدد، ترجمه خواهند شد. به روش فوق (PAT Port Address Translation) نیز گفته می شود.



- **Overlapping** . در روش فوق شبکه خصوصی از مجموعه ای IP ریجستر شده استفاده می کند که توسط شبکه دیگر استفاده می گردند. NAT می بایست آدرس های فوق را به آدرس های IP ریجستر شده منحصربفرد ترجمه نماید. NAT همواره آدرس های یک شبکه خصوصی را به آدرس های ریجستر شده منحصر بفرد ترجمه می نماید. NAT همچنین آدرس های ریجستر شده عمومی را به آدرس های منحصر بفرد در یک شبکه خصوصی ترجمه می نماید. (در هر

حالت خروجی NAT ، آدرس های IP منحصر بفرد خواهد بود. آدرس های فوق می تواند در شبکه های عمومی ریجستر شده جهانی باشند و در شبکه های خصوصی ریجستر شده محلی باشند)



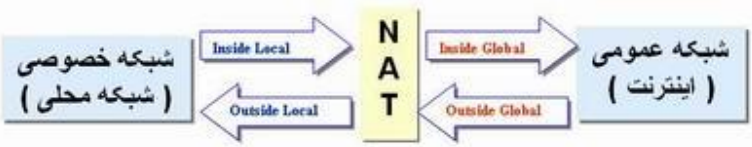
شبکه اختصاصی (خصوصی) معمولا" بصورت یک شبکه LAN می باشند.

به این نوع شبکه ها که از آدرس های IP داخلی استفاده می نمایند حوزه محلی می گویند. اغلب ترافیک شبکه در حوزه محلی بصورت داخلی بوده وبنابراین ضرورتی به ارسال اطلاعات خارج از شبکه را نخواهد داشت. یک حوزه محلی می تواند دارای آدرس های IP ریجستر شده و یا غیرریجستر شده باشد. هر کامپیوتری که از آدرس های IP غیرریجستر شده استفاده می کنند، می بایست از NAT به منظور ارتباط با دنیای خارج از شبکه محلی استفاده نمایند.

NAT می تواند با استفاده از روش های متفاوت پیکربندی گردد. در مثال زیر NAT بگونه ای پیکربندی شده است که بتواند آدرس های غیر ریجستر شده IP (داخلی و محلی) که بر روی شبکه خصوصی (داخلی) می باشند را به آدرس های IP ریجستر شده ترجمه نماید.

- یک ISP (مرکز ارائه دهنده خدمات اینترنت) یک محدوده از آدرس های IP را برای شرکت شما در نظر می گیرد. آدرس های فوق ریجستر و منحصر بفرد خواهند بود. آدرس های فوق Inside global نامیده می شوند. آدرس های IP خصوصی و غیرریچستر شده به دو گروه عمده تقسیم می گردند: یک گروه کوچک که توسط NAT استفاده شده (Outside local address) و گروه بزرگتری که توسط حوزه محلی استفاده خواهند شد(Inside local dress). آدرس های Outside local به منظور ترجمه به آدرس های منحصربفرد IP

استفاده می شوند. آدرس های منـحصر بفرد فوق، outside global نامیده شده و اختصاص به دستگاههای موجود بر روی شبکه عمومی (اینترنت) دارند.



- اکثر کامپیوترهای موجود در حوزه داخلی با استفاده از آدرس های inside local با یکدیگر ارتباط برقرار می نمایند.
- برخی از کامپیوترهای موجود در حوزه داخلی که نیازمند ارتباط دائم با خارج از شبکه باشند ،از آدرس های inside global استفاده و بدین ترتیب نیازی به ترجمه نخواهند داشت.
- زمانیکه کامپیوتر موجود در حوزه محلی که دارای یک آدرس inside local است، قصد ارتباط با خارج شبکه را داشته باشد بسته های اطلاعاتی وی در اختیار NAT قرار خواهد گرفت.
- NAT جدول روتینگ خود را بررسی تا به این اطمینان برسد که برای آدرس مقصد یک entry در اختیار دارد. در صورتی که پاسخ مثبت باشد، NAT بسته اطلاعاتی مربوطه را ترجمه و یک entry برای آن ایجاد و آن را در جدول ترجمه آدرس (ATT) ثبت خواهد کرد. در صورتی که پاسخ منفی باشد بسته اطلاعاتی دور انداخته خواهد شد.
- با استفاده از یک آدرس inside global ، روتر بسته اطلاعاتی را به مقصد مورد نظر ارسال خواهد کرد.
- کامپیوتر موجود در شبکه عمومی (اینترنت)، یک بسته اطلاعاتی را برای شبکه خصوصی ارسال می دارد. آدرس مبداء بسته اطلاعاتی از نوع outside global است . آدرس مقصد یک آدرس inside global است.

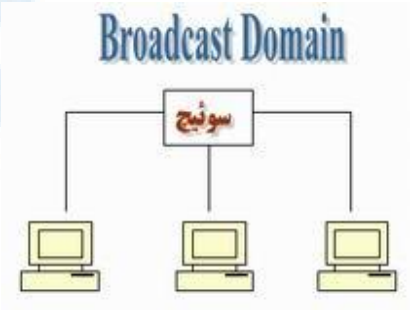
- NAT در جدول مربوطه به خود جستجو و آدرس مقصد را تشخیص و در ادامه آن را به کامپیوتر موجود در حوزه داخلی نسبت خواهد کرد.
- NAT آدرس های inside global بسته اطلاعاتی را به آدرس های inside local ترجمه و آنها را برای کامپیوتر مقصد ارسال خواهد کرد.

VLAN

VLAN (Virtual Local Area Networks)، یـکی از جدیدتـــرین و جالبترین تکنولـــوژی های شبکه است که اخـیرا" مورد توجه بیشتری قرار گرفته است. رشد بدون وقفه شبکه های LAN و ضرورت کاهش هزینه ها برای تجهیزات گرانقیمت بدون از دست دادن کارآئی و امنیت، اهمیت و ضرورت توجه بیشتر به VLAN را مضاعف نموده است.

وضعیت شبکه های فعلی

تقریبا" در اکثر شبکه ها امروزی از یک (و یا چندین) سوئیچ که تمامی گره های شبکه به آن متصل می گردند ، استفاده می شود. سوئیچ ها روشی مطمئن و سریع به منظور مبادله اطلاعات بین گره ها در یک شبکه را فراهم می نمایند.با این که سوئیچ ها برای انواع شبکه ها، گزینه ای مناسب می باشند، ولی همزمان با رشد شبکه و افزایش تعداد ایستگاهها و سرویس دهندگان، شاهد بروز مسائل خاصی خواهیم بود. سوئیچ ها، دستگاه های لایه دوم (مدل مرجع OSI) می باشند که یک شبکه Flat را ایجاد می نمایند.



همانگونه که در شکل فوق مشاهده می نمائید، به یک سوئیچ، سه ایستگاه متصل شده است. ایستگاههای فوق قادر به ارتباط با یکدیگر بوده و هر یک به عنوان عضوی از یک Broadcast domain مشابه می باشند. بدین ترتیب، در صورتی که ایستگاهی

یک پیام broadcast را ارسال نماید، سایر ایستگاههای متصل شده به سوئیچ نیز آن را دریافت خواهند داشت.

در یک شبکه کوچک، وجود پیام های Broadcast نمی تواند مشکل و یا مسئله قابل توجهی را ایجاد نماید، ولی در صورت رشد شبکه، وجود پیام های braodcast می تواند به یک مشکل اساسی و مهم تبدیل گردد. در چنین مواردی و در اغلب مواقع، سیلابی از اطلاعات بی ارزش بر روی شبکه در حال جابجائی بوده و عملا" از پهنای باند شبکه،استفاده مطلوب نخواهد شد. تمامی ایستگاههای متصل شده به یک سوئیچ، پیام های Braodcast را دریافت می نمایند. چراکه تمامی آنان بخشی از یک Broadcast doamin مشابه می باشند.

در صورت افزایش تعداد سوئیچ ها و ایستگاهها در یک شبکه، مشکل اشاره شده ملموس تر خواهد بود .همواره احتمال وجود پیام های Braodcast در یک شبکه وجود خواهد داشت.

یکی دیگر از مسائل مهم، موضوع امنیت است. در شبکه هائی که با استفاده از سوئیچ ایجاد می گردند، هر یک از کاربران شبکه قادر به مشاهده تمامی دستگاههای موجود در شبکه خواهند بود. در شبکه ای بزرگ که دارای سرویس دهندگان فایل، بانک های اطلاعاتی و سایر اطلاعات حساس و حیاتی است ، این موضوع می تواند امکان مشاهده تمامی دستگاههای موجود در شبکه را برای هر شخص فراهم نماید. بدین ترتیب منابع فوق در معرض تهدید و حملات بیشتری قرار خواهند گرفت. به منظور حفاظت اینچنین سیستم هائی می بایست محدودیت دستیابی را در سطح شبکه و با ایجاد سگمنت های متعدد و یا استقرار یک فایروال در جلوی هر یک از سیستم های حیاتی، انجام داد.

معرفی VLAN

تمامی مسائل اشاره شده در بخش قبل را و تعداد بیشتری را که به آنان اشاره نشده است را می توان با ایجاد یک VLAN به فراموشی سپرد. به منظور ایجاد VLAN،

به یک سوئیچ لایه دوم که این تکنولوژی را حمایت نماید، نیاز می باشد. تعدادی زیادی از افرادیکه جدیدا" با دنیای شبکه آشنا شده اند ، اغلب دارای برداشت مناسبی در این خصوص نمی باشند و اینگونه استنباط نموده اند که صرفا" می بایست به منظور فعال نمودن VLAN ، یک نرم افزار اضافه را بر روی سرویس گیرندگان و یا سوئیچ نصب نمایند. (برداشتی کاملا" اشتباه !). با توجه به این که در شبکه های VLAN ، میلیون ها محاسبات ریاضی انجام می شود، می بایست از سخت افزار خاصی که درون سوئیچ تعبیه شده است، استفاده گردد (دقت در زمان تهیه یک سوئیچ)،در غیر اینصورت امکان ایجاد یک VLAN با استفاده از سوئیچ تهیه شده، وجود نخواهد داشت. هر VLAN که بر روی سوئیچ ایجاد می گردد ، به منزله یک شبکه مجزا می باشد . بدین ترتیب برای هر VLAN موجود یک broadcast domain جداگانه ایجاد می گردد . پیام های broadcast ، به صورت پیش فرض، از روی تمامی پورت هائی از شبکه که عضوی از یک VLAN مشابه نمی باشند، فیلتر می گردند. ویژگی فوق، یکی از مهمترین دلایل متداول شدن VALN در شبکه های بزرگ امروزی است (تمایز بین سگمنت های شبکه). شکل زیر یک نمونه شبکه با دو VLAN را نشان می دهد:

در شکل فوق، یک شبکه کوچک با شش ایستگاه را که به یک سوئیچ (با قابلیت حمایت از VLAN) متصل شده اند، مشاهده می نمائیم. با استفاده از پتانسیل VLAN سوئیچ، دو VLAN ایجاد شده است که به هر یک سه ایستگاه متصل شده است (VLAN1 و VLAN2) .

زمانی که ایستگاه شماره یک متعلق به VLAN1 ، یک پیام Braodcast را ارسال می نماید (نظیر:FF:FF:FF:FF:FF:FF)، سوئیچ موجود آن را صرفا" برای ایستگاههای شماره دو وسه فوروارد می نماید . در چنین مواردی سایر ایستگاههای متعلق به VLAN2 ، آگاهی لازم در خصوص پیام های broadcast ارسالی بر روی VLAN1 را پیدا نکرده و درگیر این موضوع نخواهند شد.

در حقیقت ، سوئیچی که قادر به حمایت از VLAN می باشد ، امکان پیاده سازی چندین شبکه مجزا را فراهم می نماید (مشابه داشتن دو سوئیچ جداگانه و اتصال سه ایستگاه به هر یک از آنان در مقابل استفاده از VLAN). بدین ترتیب شاهد کاهش چشمگیر هزینه های برپاسازی یک شبکه خواهیم بود.

فرض کنید قصد داشته باشیم زیر ساخت شبکه موجود در یک سازمان بزرگ را به دوازده شبکه جداگانه تقسیم نمائیم. بدین منظور می توان با تهیه دوازده سوئیچ و اتصال ایستگاههای مورد نظر به هر یک از آنان ، دوازده شبکه مجزا که امکان ارتباط بین آنان وجود ندارد را ایجاد نمائیم. یکی دیگر از روش های تامین خواسته فوق، استفاده از VLAN است . بدین منظور می توان از یک و یا چندین سوئیچ که VLAN را حمایت می نمایند، استفاده و دوازده VLAN را ایجاد نمود . بدیهی است، هزینه برپاسازی چنین شبکه های به مراتب کمتر از حالتی است که از دوازده سوئیچ جداگانه، استفاده شده باشد .

در زمان ایجاد VALN، می بایست تمامی ایستگاهها را به سوئیچ متصل و در ادامه، ایستگاههای مرتبط با هر VLAN را مشخص نمود. هر سوئیچ در صورت حمایت از VLAN ، قادر به پشتیبانی از تعداد مشخصی VLAN است . مثلا" یک سوئیچ ممکن است ٦٤ و یا ٢٦٦ VLAN را حمایت نماید.

شبکه های VPN

در طی ده سال گذشته دنیا دستخوش تحولات فراوانی در عرصه ارتباطات بوده است. اغلب سازمانها و موسسات ارائه دهنده کالا و خدمات که در گذشته بسیار محدود و منطقه ای مسائل را دنبال و در صدد ارائه راهکارهای مربوطه بودند، امروزه بیش از گذشته نیازمند تفکر در محدوده جهانی برای ارائه خدمات و کالای تولیده شده را دارند. به عبارت دیگر تفکرات منطقه ای و محلی حاکم بر فعالیت های تجاری جای خود را به تفکرات جهانی و سراسری داده اند. امروزه با سازمانهای زیادی برخورد می نمائیم که در سطح یک کشور دارای دفاتر فعال و حتی در سطح دنیا دارای دفاتر متفاوتی می باشند . تمام سازمانهای فوق قبل از هر چیز بدنبال یک اصل بسیار مهم می باشند: یک روش سریع، ایمن و قابل اعتماد به منظور برقراری ارتباط با دفاتر و نمایندگی در اقصی
نقاط یک کشور و یا در سطح دنیا.

اکثر سازمانها و موسسات به منظور ایجاد یک شبکه WAN از خطوط اختصاصی (Leased Line) استفاده می نمایند.خطوط فوق دارای انواع متفاوتی می باشند. **ISDN** (با سرعت ۱۲۸ کیلوبیت در ثانیه)، (**OC3** Optical Carrier-3) (با سرعت ۱۵۵ مگابیت در ثانیه) دامنه وسیع خطوط اختصاصی را نشان می دهد. یک شبکه WAN دارای مزایای عمده ای نسبت به یک شبکه عمومی نظیر اینترنت از بعد امنیت وکارآئی است. پشتیانی و نگهداری یک شبکه WAN در عمل و زمانیکه ازخطوط اختصاصی استفاده می گردد، مستلزم صرف هزینه بالائی است.

همزمان با عمومیت یافتن اینترنت، اغلب سازمانها و موسسات ضرورت توسعه شبکه اختصاصی خود را بدرستی احساس کردند. در ابتدا شبکه های اینترانت مطرح گردیدند.این نوع شبکه بصورت کاملا" اختصاصی بوده و کارمندان یک سازمان با استفاده از رمز عبور تعریف شده ، قادر به ورود به شبکه و استفاده از منابع موجود می باشند.

اخیرا"، تعداد زیادی از موسسات و سازمانها با توجه به مطرح شدن خواسته های جدید (کارمندان از راه دور ، ادارات از راه دور)، اقدام به ایجاد شبکه های اختصاصی مجازی **VPN** (Virtual Private Network) نموده اند.

یک VPN ، شبکه ای اختصاصی بوده که از یک شبکه عمومی (عموما" اینترنت)، برای ارتباط با سایت های از راه دور و ارتباط کاربران بایکدیگر، استفاده می نماید. این نوع شبکه ها در عوض استفاده از خطوط واقعی نظیر: خطوط Leased، از یک ارتباط مجازی بکمک اینترنت برای شبکه اختصاصی به منظور ارتباط به سایت ها استفاده می کند.

عناصر تشکیل دهنده یک VPN

دو نوع عمده شبکه های VPN وجود دارد:

- **دستیابی از راه دور (Remote-Access)** . به این نوع از شبکه ها **VPDN**(network Virtual private dial-up)، نیز گفته می شود.در شبکه های فوق از مدل ارتباطی User-To-Lan (ارتباط کاربر به یک شبکه محلی) استفاده می گردد. سازمانهائی که از مدل فوق استفاده می نمایند ، بدنبال ایجاد تسهیلات لازم برای ارتباط پرسنل (عموما" کاربران از راه دور و در هر مکانی می توانند حضور داشته باشند) به شبکه سازمان می باشند. سازمانهائی که تمایل به برپاسازی یک شبکه بزرگ " دستیابی از راه دور " می باشند، می بایست از امکانات یک مرکز ارائه دهنده خدمات اینترنت جهانی **ESP**(service provider Enterprise) استفاده نمایند. سرویس دهنده ESP ، به منظور نصب و پیکربندی VPN ، یک **NAS** (Network access server) را پیکربندی و نرم افزاری را در اختیار کاربران از راه دور به منظور ارتباط با سایت قرار خواهد داد. کاربران در ادامه با برقراری ارتباط قادر به دستیابی به NAS و استفاده از نرم افزار مربوطه به منظور دستیابی به شبکه سازمان خود خواهند بود.

- **سایت به سایت (Site-to-Site)** . در مدل فوق یک سازمان با توجه به سیاست های موجود ، قادر به اتصال چندین سایت ثابت از طریق یک شبکه عمومی نظیر اینترنت است . شبکه های VPN که از روش فوق استفاده می نمایند، دارای گونه های خاصی در این زمینه می باشند:

  – مبتنی بر اینترانت . در صورتی که سازمانی دارای یک و یا بیش از یک محل (راه دور) بوده و تمایل به الحاق آنها در یک شبکه اختصاصی باشد، می توان یک اینترانت VPN را به منظور برقرای ارتباط هر یک از شبکه های محلی با یکدیگر ایجاد نمود.

  – مبتنی بر اکسترانت . در مواردیکه سازمانی در تعامل اطلاعاتی بسیار نزدیک با سازمان دیگر باشد ، می توان یک اکسترانت VPN را به منظور ارتباط شبکه های محلی هر یک از سازمانها ایجاد کرد. در چنین حالتی سازمانهای متعدد قادر به فعالیت در یک محیط اشتراکی خواهند بود.

استفاده از VPN برای یک سازمان دارای مزایای متعددی نظیر: گسترش محدوه جغرافیائی ارتباطی، بهبود وضعیت امنیت، کاهش هزینه های عملیاتی در مقایسه با روش های سنتی WAN ، کاهش زمان ارسال و حمل اطلاعات برای کاربران از راه دور، بهبود بهره وری، توپولوژی آسان ،... است. در یکه شبکه VPN به عوامل متفاوتی نظیر: امنیت، اعتمادپذیری ، مدیریت شبکه و سیاست ها نیاز خواهد بود.

شبکه های LAN جزایر اطلاعاتی

فرض نمائید در جزیره ای در اقیانوسی بزرگ ، زندگی می کنید. هزاران جزیره در اطراف جزیره شما وجود دارد. برخی از جزایر نزدیک و برخی دیگر دارای مسافت طولانی با جزیره شما می باشند. متداولترین روش به منظور مسافرت به جزیره دیگر، استفاده از یک کشتی مسافربری است . مسافرت با کشتی مسافربری، بمنزله عدم وجود امنیت است.

در این راستا هر کاری را که شما انجام دهید ، توسط سایر مسافرین قابل مشاهده خواهد بود. فرض کنید هر یک از جزایر مورد نظر به مشابه یک شبکه محلی (LAN) و اقیانوس مانند اینترنت باشند. مسافرت با یک کشتی مسافربری مشابه برقراری ارتباط با یک سرویس دهنده وب و یا سایر دستگاههای موجود در اینترنت است. شما دارای هیچگونه کنترلی بر روی کابل ها و روترهای موجود در اینترنت نمی باشید. (مشابه عدم کنترل شما به عنوان مسافر کشتی مسافربری بر روی سایر مسافرین حاضر در کشتی). در صورتی که تمایل به ارتباط بین دو شبکه اختصاصی از طریق منابع عمومی وجود داشته باشد، اولین مسئله ای که با چالش های جدی برخورد خواهد کرد ، امنیت خواهد بود. فرض کنید، جزیره شما قصد ایجاد یک پل ارتباطی با جزیره مورد نظر را داشته باشد .مسیر ایجاد شده یک روش ایمن، ساده و مستقیم برای مسافرت ساکنین جزیره شما به جزیره دیگر را فراهم می آورد. همانطور که حدس زده اید ، ایجاد و نگهداری یک پل ارتباطی بین دو جزیره مستلزم صرف هزینه های بالائی خواهد بود.(حتی اگر جزایر در مجاورت یکدیگر باشند). با توجه به ضرورت و حساسیت مربوط به داشتن یک مسیر ایمن و مطمئن، تصمیم به ایجاد پل ارتباطی بین دو جزیره گرفته شده است. در صورتی که جزیره شما قصد ایجاد یک پل ارتباطی با جزیره دیگر را داشته باشد که در مسافت بسیار طولانی نسبت به جزیره شما واقع است

، هزینه های مربوط بمراتب بیشتر خواهد بود. وضعیت فوق، نظیر استفاده از یک اختصاصی Leased است. ماهیت پل های ارتباطی (خطوط اختصاصی) از اقیانوس (اینترنت) متفاوت بوده و کماکن قادر به ارتباط جزایر(شبکه های LAN) خواهند بود. سازمانها و موسسات متعددی از رویکرد فوق (استفاده از خطوط اختصاصی) استفاده می نمایند. مهمترین عامل در این زمینه وجود امنیت و اطمینان برای برقراری ارتباط هر یک سازمانهای مورد نظر با یکدیگر است. در صورتی که مسافت ادارات و یا شعب یک سازمان از یکدیگر بسیار دور باشد، هزینه مربوط به برقرای ارتباط نیز افزایش خواهد یافت.

با توجه به موارد گفته شده، چه ضرورتی به منظور استفاده از VPN وجود داشته و VPN تامین کننده، کدامیک از اهداف و خواسته های مورد نظر است؟ با توجه به مقایسه انجام شده در مثال فرضی، می توان گفت که با استفاده از VPN به هریک از ساکنین جزیره یک زیردریائی داده می شود. زیردریائی فوق دارای خصایص متفاوت نظیر :

- دارای سرعت بالا است.
- هدایت آن ساده است.
- قادر به استتار(مخفی نمودن) شما از سایر زیردریا ئیها و کشتی ها است.
- قابل اعتماد است .
- پس از تامین اولین زیردریائی ، افزودن امکانات جانبی و حتی یک زیردریائی دیگرمقرون به صرفه خواهد بود

در مدل فوق، با وجود ترافیک در اقیانوس، هر یک از ساکنین دو جزیره قادر به تردد در طول مسیر در زمان دلخواه خود با رعایت مسایل ایمنی می باشند. مثال فوق دقیقا" بیانگر تحوه عملکرد VPN است. هر یک از کاربران از راه دور شبکه قادربه برقراری ارتباطی امن و مطمئن با استفاده از یک محیط انتقال عمومی (نظیر اینترنت) با شبکه محلی (LAN) موجود در سازمان خود خواهند بود. توسعه یک VPN (افزایش تعداد کاربران از راه دور و یا افزایش مکان های مورد نظر) بمراتب آسانتر از شبکه هائی است که از خطوط اختصاصی استفاده می نمایند. قابلیت توسعه فراگیر از مهمتزین ویژگی های یک VPN نسبت به خطوط اختصاصی است.

امنیت VPN

شبکه های VPN به منظور تامین امنیت (داده ها و ارتباطات) از روش های متعددی استفاده می نمایند:

- **فایروال** . فایروال یک دیواره مجازی بین شبکه اختصای یک سازمان و اینترنت ایجاد می نماید. با استفاده از فایروال می توان عملیات متفاوتی را در جهت اعمال سیاست های امنیتی یک سازمان انجام داد. ایجاد محدودیت در تعداد پورت ها فعال ، ایجاد محدودیت در رابطه به پروتکل های خاص ، ایجاد محدودیت در نوع بسته های اطلاعاتی و ... نمونه هائی از عملیاتی است که می توان با استفاده از یک فایروال انجام داد.
- **رمزنگاری** . فرآیندی است که با استفاده از آن کامپیوتر مبداء اطلاعاتی رمزشده را برای کامپیوتر دیگر ارسال می نماید. سایر کامپیوترها ی مجاز قادر به رمزگشائی اطلاعات ارسالی خواهند بود. بدین ترتیب پس از ارسال اطلاعات توسط فرستنده، دریافت کنندگان، قبل از استفاده از اطلاعات می بایست اقدام به رمزگشائی اطلاعات ارسال شده نمایند. سیستم های رمزنگاری در کامپیوتر به دو گروه عمده تقسیم می گردد: رمزنگاری کلید متقارن و رمزنگاری کلید عـــمومی در رمز نگاری " کلید متقارن " هر یک از کامپیوترها دارای یک کلید Secret (کد) بوده که با استفاده از آن قادر به رمزنگاری یک بسته اطلاعاتی قبل از ارسال در شبکه برای کامپیوتر دیگر می باشند. در روش فوق می بایست در ابتدا نسبت به کامپیوترهائی که قصد برقراری و ارسال اطلاعات برای یکدیگر را دارند، آگاهی کامل وجود داشته باشد. هر یک از کامپیوترهای شرکت کننده در مبادله اطلاعاتی می بایست دارای کلید رمز مشابه به منظور رمزگشائی اطلاعات باشند. به منظور رمزنگاری اطلاعات ارسالی نیز از کلید فوق استفاده خواهد شد. فرض کنید قصد ارسال یک پیام رمز شده برای یکی از دوستان خود را داشته باشید. بدین منظور از یک الگوریتم خاص برای رمزنگاری استفاده می شود. در الگوریتم فوق هر حرف به دوحرف بعد از خود تبدیل می گردد. (حرف A به حرف C ، حرف B به حرف D). پس از رمزنمودن پیام و ارسال آن، می بایست دریافت کننده پیام به این حقیقت واقف باشد که برای رمزگشائی پیام لرسال شده، هر حرف به دو حرق قبل از خود می بایست تبدیل گردد.

در چنین حالتی می بایست به دوست امین خود، واقعیت فوق (کلید رمز) گفته شود. در صورتی که پیام فوق توسط افراد دیگری دریافت گردد، بدلیل عدم آگاهی از کلید، آنان قادر به رمزگشائی و استفاده از پیام ارسال شده نخواهند بود.

در رمزنگاری عمومی از ترکیب یک کلید خصوصی و یک کلید عمومی استفاده می شود. کلید خصوصی صرفا" برای کامپیوتر شما (ارسال کننده) قابل شناسائی و استفاده است. کلید عمومی توسط کامپیوتر شما در اختیار تمام کامپیوترهای دیگر که قصد ارتباط با آن را داشته باشند ، گذاشته می شود. به منظور رمزگشائی یک پیام رمز شده، یک کامپیوتر می بایست با استفاده از کلید عمومی (ارائه شده توسط کامپیوتر ارسال کننده) ، کلید خصوصی مربوط به خود اقدام به رمزگشائی پیام ارسالی نماید . یکی از متداولترین ابزار "رمزنگاری کلید عمومی"، روشی با نام Pretty Good Privacy(PGP) است.

با استفاده از روش فوق می توان اقدام به رمزنگاری اطلاعات دلخواه خود نمود.

- **IPSec** . پروتکل protocol Internet protocol security(IPsec) ، یکی از امکانات موجود برای ایجاد امنیت در ارسال و دریافت اطلاعات می باشد . قابلیت روش فوق در مقایسه با الگوریتم های رمزنگاری بمراتب بیشتر است. پروتکل فوق دارای دو روش رمزنگاری است : Tunnel، Transport . در روش tunel ، هدر و Payload رمز شده درحالیکه در روش transport صرفا" payload رمز می گردد. پروتکل فوق قادر به رمزنگاری اطلاعات بین دستگاههای متفاوت است:
  - روتر به روتر
  - فایروال به روتر
  - کامپیوتر به روتر
  - کامپیوتر به سرویس دهنده

- **سرویس دهنده AAA** . سرویس دهندگان(**AAA** : Authentication ،Authorization,Accounting) به منظور ایجاد امنیت بالا در محیط هـای VPN از نوع " دستیابی از راه دور " استفاده می گردند. زمانیکه کاربران با استفاده از خط تلفن به سیستم متصل می گردند ، سرویس دهنده AAA درخواست آنها را اخذ و عمایات زیر را انجام خواهد داد :
  - شما چه کسی هستید؟ (تایید، Authentication)
  - شما مجاز به انجام چه کاری هستید؟ (مجوز، Authorization)
  - چه کارهائی را انجام داده اید؟ (حسابداری، Accounting)

تکنولوژی های VPN

با توجه به نوع VPN (" دستیابی از راه دور " و یا " سایت به سایت ") ، به منظور ایجاد شبکه از عناصر خاصی استفاده می گردد:

- نرم افزارهای مربوط به کاربران از راه دور
- سخت افزارهای اختصاصی نظیر یک " کانکتور VPN" و یا یک فایروال PIX
- سرویس دهنده اختصاصی VPN به منظور سرویُس های Dial-up
- سرویس دهنده NAS که توسط مرکز ارائه خدمات اینترنت به منظور دستیابی به VPN از نوع "دستیابی از را دور" استفاده می شود.
- شبکه VPN و مرکز مدیریت سیاست ها

با توجه به اینکه تاکنون یک استاندارد قابل قبول و عمومی به منظور ایجاد شVPN ایجاد نشده است، شرکت های متعدد هر یک اقدام به تولید محصولات اختصاصی خود نموده اند.

- **کانکتور VPN** . سخت افزار فوق توسط شرکت سیسکو طراحی و عرضه شده است. کانکتور فوق در مدل های متفاوت و قابلیت های گوناگون عرضه شده است . در برخی از نمونه های دستگاه فوق امکان فعالیت همزمان ۱۰۰ کاربر از

راه دور و در برخی نمونه های دیگر تا ۱۰،۰۰۰ کاربر از راه دور قادر به اتصال به شبکه خواهند بود.

- **روتر مختص VPN** . روتر فوق توسط شرکت سیسکو ارائه شده است. این روتر دارای قابلیت های متعدد به منظور استفاده در محیط های گوناگون است.

در طراحی روتر فوق شبکه های VPN نیز مورد توجه قرار گرفته و امکانات مربوط در آن بگونه ای بهینه سازی شده اند.

- **فایروال PIX** . (فایروال PIX (eXchange Private Internet قابلیت هائی نظیر NAT، سرویس دهنده Proxy، فیلتر نمودن بسته ای اطلاعاتی، فایروال و VPN را در یک سخت افزار فراهم نموده است.

Tunneling(تونل سازی)

اکثر شبکه های VPN به منظور ایجاد یک شبکه اختصاصی با قابلیت دستیابی از طریق اینترنت از امکان " Tunneling " استفاده می نمایند. در روش فوق تمام بسته اطلاعاتی در یک بسته دیگر قرار گرفته و از طریق شبکه ارسال خواهد شد. پروتکل مربوط به بسته اطلاعاتی خارجی (پوسته) توسط شبکه و دو نقطه (ورود و خروج بسته اطلاعاتی) قابل فهم می باشد. دو نقطه فوق را "اینترفیس های تونل " می گویند.

روش فوق مستلزم استفاده از سه پروتکل است:

- پروتکل حمل کننده . از پروتکل فوق شبکه حامل اطلاعات استفاده می نماید.
- پروتکل کپسوله سازی . از پروتکل هائی نظیر:

  IPSec,L2F,PPTP,L2TP,GRE استفاده می گردد.
- پروتکل مسافر . از پروتکل هائی نظیر IPX,IP,NetBeui به منظور انتقال داده های اولیه استفاده می شود.

با استفاده از روش Tunneling می توان عملیات جالبی را انجام داد. مثلا" می توان از بسته ای اطلاعاتی که پروتکل اینترنت را حمایت نمی کند (نظیر NetBeui) درون یک بسته اطلاعاتی IP استفاده و آن را از طریق اینترنت ارسال نمود

و یا می توان یک بسته اطلاعاتی را که از یک آدرس IP غیر قابل روت (اختصاصی) استفاده می نماید ، درون یک بسته اطلاعاتی که از آدرس های معتبر IP استفاده می کند، مستقر و از طریق اینترنت ارسال نمود.

در شبکه های VPN از نوع " سایت به سایت " ، **GRE** (generic routing encapsulation) به عنوان پروتکل کپسوله سازی استفاده می گردد. فرآیند فوق نحوه استقرار و بسته بندی " پروتکل مسافر" از طریق پروتکل " حمل کننده " برای انتقال را تبین می نماید. (پروتکل حمل کننده ، عموما" IP است). فرآیند فوق شامل اطلاعاتی در رابطه با نوع بست های اطلاعاتی برای کپسوله نمودن و اطلاعاتی در رابطه با ارتباط بین سرویس گیرنده و سرویس دهنده است. در برخی موارد از پروتکل IPSec (در حالت tunnel) برای کپسوله سازی استفاده می گردد.پروتکل IPSec ، قابل استفاده در دو نوع شبکه VPN (سایت به یایت و دستیابی از راه دور) است. اینترفیش های Tunnel می بایست دارای امکانات حمایتی از IPSec باشند.

در شبکه های VPN از نوع " دستیابی از راه دور " ، Tunneling با استفاده از PPP انجام می گیرد. PPP به عنوان حمل کننده سایر پروتکل های IP در زمان برقراری ارتباط بین یک سیستم میزبان و یک سیستم ازه دور ، مورد استفاده قرار می گیرد. هر یک از پروتکل های زیر با استفاده از ساختار اولیه PPP ایجاد و توسط شبکه های VPN از نوع " دستیابی از راه دور " استفاده می گردند:

- **Layer 2 Forwarding(F۲L)** . پروتکل فوق توسط سیسکو ایجاد شده است . در پروتکل فوق از مدل های تعیین اعتبار کاربر که توسط PPP حمایت شده اند ، استفاده شد ه است.
- **Point-to-Point Tunneling Protocol(PPTP)** . پروتکل فوق توسط کنسرسیومی متشکل از شرکت های متفاوت ایجاد شده است. این پروتکل امکان رمزنگاری ٤٠ بیتی و ١٢٨ بیتی را دارا بوده و از مدل های تائید اعتبار کاربر که توسط PPP حمایت می گردد ، استفاده می نماید.

- **Layer 2 Tunneling Protocol(L2TP)** . پروتکل فوق با همکاری چندین شرکت ایجاد شده است. پروتکل فوق از ویژگی های PPTP و L2F استفاده کرده است. پروتکل L2TP بصورت کامل IPSec را حمایت می کند.

از پروتکل فوق به منظور ایجاد تونل بین موارد زیر استفاده می گردد :

- سرویس گیرنده و روتر
- NAS و روتر
- روتر و روتر

عملکرد Tunneling مشابه حمل یک کامپیوتر توسط یک کامیون است . فروشنده ، پس از بسته بندی کامپیوتر (پروتکل مسافر) درون یک جعبه (پروتکل کپسوله سازی) آن را توسط یک کامیون (پروتکل حمل کننده) از انبار خود (اینترفیس ورودی تونل) برای متقاضی ارسال می دارد.

کامیون (پروتکل حمل کننده) از طریق بزرگراه (اینترنت) مسیر خود را طی، تا به منزل شما (اینترفیش خروجی تونل) برسد. شما در منزل جعبه (پروتکل کپسول سازی) را باز و کامپیوتر (پروتکل مسافر) را از آن خارج می نمائید.

اشتراک منابع

یکی از اهداف اولیه و مهم دربرپاسازی شبکه های کامپیوتری ،اشتراک منابع است. منابع موجود در کامپیوتر به دو گروه عمده منابع فیزیکی (چاپگر) و منابع منطقی (فایل ها) تقسیم می گردند. پس از ایجاد یک شبکه می توان با توجه به بستر ایجاد شده عملیات متفاوتی را انجام داد:

- اشتراک یک چاپگر به منظور استفاده توسط کامپیوترهای موجود در شبکه
- استفاده از یک خط ارتباطی اینترنت توسط کامپیوترهای موجود در شبکه
- اشتراک فایل ها ی اطلاعاتی با محتویات متفاوت
- استفاده از بازیهای کامپیوتری که چندین کاربر بصورت همزمان می توانند از آن استفاده نمایند.
- ارسال خروجی دستگاههائی نظیر دوربین های وب برای سایر کامپیوترهای موجود درشبکه

به منظور بر پا سازی یک شبکه کامپیوتری کوچک، می بایست مراحل زیر را دنبال نمود :

- **انتخاب تکنولوژی مورد نظر جهت استفاده در شبکه** . اترنت به عنوان مهمترین تکنولوژی در این راستا مطرح است.
- **تهیه و نصب سخت افزارهای مربوطه**. هر یک از کامپیوترهای موجود در شبکه می بایست دارای یک کارت شبکه باشند.در صورت استفاده از توپولوژی ستاره (در حال حاضر متداولترین نوع توپولوژی است) می بایست از یکدستگاه هاب و در موارد حرفه ای تر از یک دستگاه سوئیچ استفاده کرد. پس از نصب و پیکربندی هر یک از کارت های شبکه در کامپیوترهای مورد نظر، با استفاده از کابل های مربوطه (عموما" از کابل بهم تابیده Cat5 استفاده می گردد) هر یک از کامپیوترها به هاب و یا سوئیچ متصل می گردند.

- **پیکربندی سیستم به منظور استفاده از منابع مشترک در سیستم** : این مرحـــله (پیکربندی سیستم)، یکی از مراحل مهم در زمینه آماده سازی شبـــــکه برای استفاده توسط کاربران است.ر این مرحله می بایست عملیات زیرصورت پذیرد:

– نامگذاری کامپیوتر

– اشتراک فایل ها

– اشتراک چاپگر

– امنیت

– اشتراک خط اینترنت

در ادامه به بررسی نحوه انجام هر یک از عملیات فوق خواهیم پرداخت.

نامگذاری کامپیوتر

قبل از اینکه کامپیوتری به عنوان یکی از گره های شبکه مطرح گردد، می بایست برای آن نام و یک گروه را مشخص کرد. هر یک از کامپیوترهای موجود در شبکه می بایست دارای یک نام منحصر بفرد و یک نام گروه یکسان باشند. برای مشخص نمودن نام کامپیوتر و گروه، عملیات زیر را می بایست انجام داد.

- **مرحله اول** : در کامپیوترهائی با سیستم عامل ویندوز ۹۸ و یا میلینیوم، موس را برروی Network Neighborhood (موجود بر روی صفحه اصلی) قرارداده و کلید سمت راست موس را فعال نمائید.
- **مرحله دوم** : گزینه Properties را از طریق منوی دستورات انتخاب نمائید. در ادامه پنجره Network Properties فعال می گردد. در پنجره فوق اطلاعاتی در رابطه با آدپتورهای شبکه و پروتکل های نصب شده بر روی کامپیوتر، نمایش داده می شود.

- **مرحله سوم** : پس از فعال شده پنجره اشاره شده، گزینه Identification را انتخاب نمائید. در این حالت سه فیلد اطلاعاتی نمایش داده می شود.
- **مرحله چهارم** : دراولین فیلد اطلاعاتی ، نام مورد نظر خود را برای کامپیوتر وارد نمائید. نام در نظر گرفته شده کاملا" انتخابی است و تنها محدودیت موجود، تکراری نبودن آن است. سایر کامپیوترهای موجود در شبکه نباید از نام فوق استفاده کرده باشند.
- **مرحله پنجم** : دردومین فیلد اطلاعاتی ، نام در نظر گرفته شده برای گروه را وارد نمائید. تمام کامپیوترهای موجود در شبکه که قصد به اشتـــــــراک گذاشتن منابع سخت افزاری و نرم افزاری بین خود را دارند ، می بایست دارای نام گروه مشابه و یکسان باشند.

اشتراک فایل و امنیت

یکی از مهمترین عملیات در هر شبکه کامپیوتری، اشتراک فایل ها است. در سیستم هائی که از ویندوز ۹۸ و یا میلینیوم استفاده می نمایند، فرآیند فوق بسادگی انجام خواهد شد. پس از پیکربندی مناسب، هر یک از کامپیوترهای موجود در شبکه قادر به اشتراک فایل بین خود خواهند بود.

به منظور فعال نمودن ویژگی فوق در ابتدا می بایست از فعال شدن گزینه File and Printer Sharing مطمئن گردید. بدین منظور موس را برروی امکان Network

Neighborhood (موجود بر روی صفحه اصلی) قرارداده و کلید سمت راست موس را فعال نمائید.گزینه Properties را از طریق منوی دستورات انتخاب نمائید. در ادامه پنجره Network Properties فعال می گردد.

در ادامه گزینه Configuration فعال و در بخش پایین پنجره فوق، امکان Client for Microsoft Networks می بایست مشاهده گردد. زمانیکه کامپیوتری به عنوان یک سرویس گیرنده (Client) در شبکه ای مطرح باشد، قادر به تبادل اطلاعاتی با سایر کامپیوترهای موجود در شبکه خواهد بود. زمانیکه عملیات مربوط به پیکربندی و تنظیم شبکه در ویندوزهای ۹۸ و یا میلینیوم انجام می گیرد، امکان اشاره شده بصورت اتوماتیک در سیستم اضافه خواهد گردید. در صورتی که امکان فوق بصورت اتوماتیک اضافه نشده باشد، می توان با دنبال نمودن مراحل زیر، آن را نصب نمود.

- **مرحله اول** : گزینه Add را از طریق پنجره Properties Network انتخاب نمائید
- **مرحله دوم** : گزینه Client را از لیست بنمایش در آمده انتخاب نمائید.
- **مرحله سوم** : با فعال کردن گزینه Add لیستی از شرکت ها و تولید کنندگان متفاوت را در پانل سمت چپ مشاهده می نمائید.

- **مرحله چهارم** : گزینه Microsoft را از طریق پانل سمت چپ انتخاب و در ادامه لیستی از نرم افزارهای سرویس گیرنده مایکروسافت در پانل سمت راست نمایش داده خوواهند شد.
- **مرحله پنجم** : از لیست فوق، گزینه Client for Microsoft Networks را انتخاب و دکمه OK را فعال نمائید. در ادامه سیستم عامل ویندوز تمام فایل های ضروری و مورد نیاز را بر روی کامپیوتر قرار خواهد داد(در این مرحله CD مربوط به ویندوز نیاز خواهد بود)

پس از نصب نرم افزارهای مورد نیاز، می توان عملیات مربوط به اشتراک فایل ها را دنبال نمود. بدین منظور در پنجره اصلی (Network) شبکه مستفر شده و مراحل زیر را دنبال نمائید:

- **مرحله اول** : دکمه مربوط به File and print sharing را فعال نمائید

- **مرحله دوم** : در این مرحله دو حق انتخاب وجود دارد. یکی برای اشتراک فایل ها و دیگری برای اشتراک چاپگر. با توجه به وضعیت موجود شبکه می توان یک و یا هر دو آیتم را انتخاب کرد.
- **مرحله سوم** : پس از انتخاب هر یک از گزینه های مورد نظر (فایل ، چاپگر)، یک Checkmark در کنار گزینهFile and print sharing فعال خواهد شد. با فعال نمودن دکمه OK پنجره مربوط به Sharing-options بسته خواهد شد.
- **مرحله چهارم** : در ادامه امکان Access Control را از طریق پنجره Network انتخاب نمائید. به منظور کنترل ساده در رابطه با هویت افرادیکی

می توانند از فایل ها استفاده نمایند، گزینه Share-level Access Control را انتخاب نمائید.

- **مرحله پنجم** : با فعال کردن دکمه OK ، پنجره Network بسته خواهد شد.

در ادامه می بایست فولدرهائی را که قصد به اشتراک گذاشتن آنها را دارید، مشخص نمائید. با ایجاد فولدرهای دلخواه و استقرار فایل های مورد نظر درهر یک می توان یک انظباط اطلاعاتی از بعد ذخیره سازی را ایجاد کرد. برای به اشتراک گذاشتن یک فولدر ، بر روی فولدر فوق مستقر و کلید سمت راست موس را فعال نمائید. گزینه Sharing را از طریق منوی مربوطه انتخاب نمائید. در ادامه پنجره ای فعال می گردد که در آن امکان انتخاب چندین آیتم وجود دارد. مقدار پیش فرض برای Sharing بصورت Not Shared است. با تغییر مقدار گزینه فوق و تبدیل آن به Shared As می توان در فیلد اطلاعاتی Name Share ، نام دلخواه خود را برای فولدر به اشتراک گذاشته شده مشخص نمود. نام فوق می تواند با نام واقعی فولدر کاملا" متفاوت می باشد. در صورتی که قبلا" گزینه Share-level Access Control را انتخاب کرده باشید ، می بایست در ادامه سطح مورد نظر امنیتی (Access Type) را مشخص و برای آن یک رمز عبور را نیز مشخص نمود. دستیابی به روش Read-only بدین مفهوم است که هر کاربر قادر به دستیابی به فولدر از طریق شبکه بوده و صرفا" قادر به مشاهده و بازیابی فایل ها خواهد بود. این نوع کاربران قادر به استقرار فایل های جدید در فولدر و یا حذف و اصلاح فایل های موجود در فولدر نخواهند بود. در صورتی که روش دستیابی به فولدر، access Full تعیین گردد، کاربران قادر به مشاهده، نوشتن، ایجاد و حذف فایل در فولدر مورد نظر خواهند بود. با توجه به نوع رمز عبور می توان هر دو گزینه را بصورت شناور نیز استفاده نمود.

اشتراک چاپگر

به منظور اشتراک یک چاپگر در ابتدا می بایست از صحت عملیات اشاره شده خصوصا" فعال شدن Sharing File and Printer اطمینان حاصل کرد. در ادامه با دنبـــال نمودن مراحل زیر می توان برای به اشتراک گذاشتن یک چاپگر مراحل زیر را دنـــبال نمود.

- **مرحله اول** : از طریق دکمه Start ، گزینه Setting و در ادامه Printers را انتخاب نمائید.در ادامه پنجره ای شامل لیستی از تمام چاپگرهای محلی نمایش داده خواهد شد.
- **مرحله دوم** : موس را بر روی آیکون چاپگری که قصد به اشتراک گذاشتن آن را دارید، قرار داده و کلید سمت راست موس را فعال و گزینه Sharing را انتخاب نمائید.
- **مرحله سوم** : در ادامه پنجره Properties فعال می گردد. در فیلد اطلاعاتی Shared As نام دلخواه برای چاپگر (به منظور اشتراک گذاشتن) را مشخص نمائید. در صورت تمایل یک رمز عبور نیز را در این مرحله مشخص نمود.

- **مرحله چهارم** : با فعال کردن دکمه OK، پنجره مربوطه بسته شده و چاپگر به اشتراک گذاشته شده است .

به منظور دستیابی به چاپگر به اشتراک گذاشته شده از طریق کامپیوترهای دیگر ، مراحل زیر را دنبال نمائید:

- **مرحله اول** : پنجره مربوط به Printer را فعال نمائید.
- **مرحله دوم** : ویزارد(برنامه کمکی) Add a Printer را فعال نمائید.
- **مرحله سوم** : گزینه Network Printer را انتخاب و دکمه OK را فعال نمائید.
- **مرحله چهارم** : ویزارد مربوطه در ادامه لیستی از چاپگرهای به اشتراک گذاشته شده موجود بر روی شبکه را نمایش خواهد داد. در ادامه چاپگر مورد نظر را انتخاب و دکمه Next را فعال نمائید. در نهایت ویزارد مربوطه درایور مورد نظر را نصب خواهد کرد. (در برخی حالات ممکن است نیاز به CD و یا دیسکت حاوی درایور چاپگر وجود داشته باشد)

اشتراک خط اینترنت

با توجه به رشد شبکه ها ی کوچک، شرکت مایکروسافت از نسخه ویندوز CE۹۸ به بعد امکانی با نام ICS(Internet Connection Sharing) را اضافه نموده است. با استفاده از ICS می توان یک کامپیوتر را که با استفاده از یکی از روش های رایج نظیر: مودم، DSL، ISDN و یا کابل به اینترنت متصل است، به اشتراک گذاشت. ویندوز CE۹۸ و سایر نسخه های ویندوز دارای یک ویزارد به منظور فعال کردن امکان فوق می باشند. عناصر نرم افزاری مورد نیاز ICS بصورت پیش فرض بر روی کامپیوتر نصب نمی گردند. توجه داشته باشید که امکان فوق صرفا" می بایست بر روی کامپیوتری که به اینترنت متصل است، فعال گردد. برای فعال نمودن امکان فوق (بر روی کامپیوترهائی که از نسخه ویندوز CE۹۸ استفاده می نمایند) می بایست مراحل زیر را دنبال کرد:

- **مرحله اول** : از طریق Control Panel ،گزینهPrograms Add/Remove را انتخاب نمائید.
- **مرحله دوم** : گزینه windows setup را انتخاب و در ادامه آیتم Internet Tools را انتخاب نمائید.
- **مرحله سوم** : عنصر Internet Connection Sharing را انتخاب نمائید. در ادامه کلید Next را فعال نمائید. در صورتی که ICS پیکربندی نشده باشد، برنامه کمکی (ویزارد) مربوط به ICS فعال و در ادامه می توان عملیات پیکربندی لازم را انجام داد.
- **مرحله چهارم** : پس از اخذ اطلاعات ضروری در رابطه با کامپیوتری که ICS بر روی آن فعال شده است، ویزارد مربوطه نیاز به یک عدد دیسکت خواهد داشت. از اطلاعات ذخیره شده بر روی دیسکت فوق به منظور پیکربندی سایر کامپیوترهای موجود در شبکه که تمایل به استفاده از سرویس ICS را داشته باشند استفاده می گردد.

مراحل فعال نمودن سرویس ICS در کامپیوترهائی که از ویندوز ۲۰۰۰ و یا XP استفاده می نمایند بمراتب راحت تر از مراحل گفته شده فوق است .در این راستا پس از ایجاد یک Dial-up ، با انتخاب آن و فعال کردن کلید سمت راست، گزینه Properties را انتخاب نمائید. در ادامه پنجره Dial-up Connection properties نمایش داده می شود.

برای اشتراک خطی ارتباط گزینه "Sharing" را انتخاب نمائید. در ادامه گزینه "Enable internet connection sharing for this connection" را انتخاب و سایر موارد و عملیات مورد نیاز بصورت اتوماتیک انجام خواهد شد.

هاب و نحوه عملکرد آن

هاب از جمله تجهیزات سخت افزاری است که از آن به منظور برپاسازی شبکه های کامپیوتری استفاده می شود . گرچه در اکثر شبکه هائی که امروزه ایجاد می گردد از سوئیچ در مقابل هاب استفاده می گردد، ولی ما همچنان شاهد استفاده از این نوع تجهیزات سخت افزاری در شبکه های متعددی می باشیم. قبل از پرداختن به اصل موضوع، لازم است در ابتدا با برخی تعاریف مهم که در ادامه بدفعات به آنان مراجعه خواهیم کرد بیشتر آشنا شویم.

- **Domain** : تمامی کامپیوترهای عضوء یک domain هر اتفاق و یا رویدادی را که در domain اتفاق می افتد، مشاهده و یا خواهند شنید.
- **Collision Domain** : در صورت بروز یک تصادم (Collision) بین دو کامپیوتر، سایر کامپیوترهای موجود در domain آن را شنیده و آگاهی لازم در خصوص آن چیزی که اتفاق افتاده است را پیدا خواهند کرد . کامپیوترهای فوق عضوء یک Collision Domain یکسان می باشند. تمامی کامپیوترهائی که با استفاده از هاب به یکدیگر متصل می شوند، عضوء یک Collision Domain یکسان خواهند بود (بر خلاف سوئیچ).
- **Broadcast Domain** : در این نوع domain، یک پیام broadcast (یک فریم و یا داده که برای تمامی کامپیوترها ارسال می گردد) برای هر یک از کامپیوترهای موجود در doamin ارسال می گردد. هاب و سوئیچ با موضوع broadcast domain برخورد مناسبی نداشته (ایجاد حوزه های مجزاء) و در این رابطه به یک روتر نیاز خواهد بود.

به منظور برخورد مناسب (ایجاد حوزه های مجزاء) با collision domain، broadcast domain و افزایش سرعت و کارائی یک شبکه از تجهیزات سخت افزاری متعددی استفاده می شود. سوئیچ ها collision domain مجزائی را ایجاد

می نمایند ولی در خصوص broadcast doamin بدین شکل رفتار نمی نمایند. روترها، broadcast domain و domain collision مجزائی را ایجاد نموده و در مقابل هاب، قادر به ایجاد broadcast doamin و domain Collision جداگانه نمی باشد. شکل زیر یک نمونه هاب هشت پورت را نشان می دهد (D-Link DE-808TP 10Mbps Ethernet 8-Port Mini-Hub).

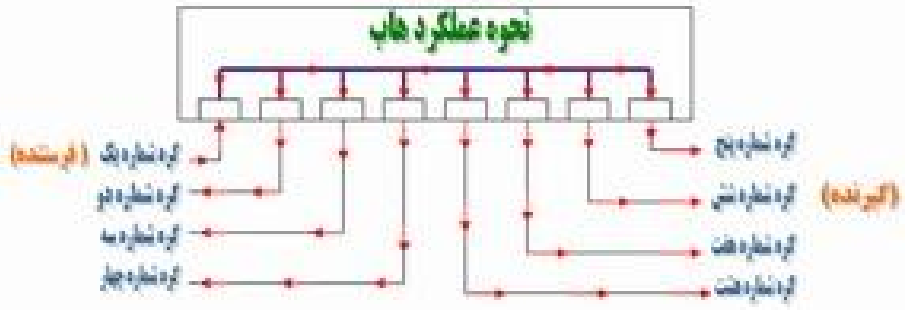
آشنائی با نحوه عملکرد هاب

هاب، یکی از تجهیزات متداول در شبکه های کامپیوتری و ارزانترین روش اتصال دو و یا چندین کامپیوتر به یکدیگر است. هاب در اولین لایه مدل مرجع OSI فعالیت می نماید. آنان فریم های داده را نمی خوانند (کاری که سوئیچ و یا روتر انجام می دهند) و صرفا" این اطمینان را ایجاد می نمایند که فریم های داده بر روی هر یک از پورت ها، تکرار خواهد شد.

گره هائی که یک اترنت و یا Fast Ethernet را با استفاده از قوانین CSMA/CD به اشتراک می گذارند ، عضوء یک Collision Domain مشابه می باشند. این بدان معنی است که تمامی گره های متصل شده به هاب بخشی از Collision domain مشابه بوده و زمانی که یک collision اتفاق می افتد، سایر گره های موجود در domain نیز آن را شنیده و از آن متاثر خواهند شد.کامپیوترها و یا گره های متصل شده به هاب از کابل های UTP (Unshielded Twisted Pair)، استفاده می نمایند. صرفا" یک گره می تواند به هر پورت هاب متصل گردد. مثلا" با استفاده از یک هاب هشت پورت، امکان اتصال هشت کامپیوتر وجود خواهد داشت. زمانی که

هاب ها به متداولی امروز نبودند و قیمت آنان نیز گران بود، در اکثر شبکه های نصب شده در ادارات و یا منازل از کابل های کواکسیال، استفاده می گردید.

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

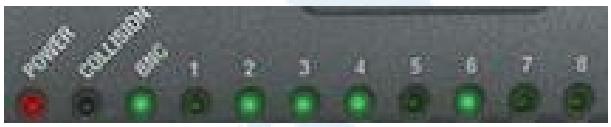


همانگونه که در شکل فوق مشاهده می نمائید، گره یک داده ئی را برای گره شش ارسال می نماید ولی تمامی گره های دیگر نیز داده را دریافت خواهند کرد. در ادامه، بررسی لازم در خصوص داده ارسالی توسط هر یک از گره ها انجام و در صورتی که تشخیص داده شود که داده ارسالی متعلق به آنان نیست، آن را نادیده خواهند گرفت. عملیات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

اکثر هاب ها دارای یک پورت خاص می باشند که می تواند به صورت یک پورت معمولی و یا یک پورت uplink رفتار نماید. با استفاده از یک پورت uplink می توان یک هاب دیگر را به هاب موجود، متصل نمود. بدین ترتیب تعداد پورت ها افزایش یافته و امکان اتصال تعداد بیشتری کامپیوتر به شبکه فراهم می گردد.

روش فوق گزینه ای ارزان قیمت به منظور افزایش تعداد گره ها در یک شبکه است ولی با انجام این کار شبکه شلوغ تر شده و همواره بر روی آن حجم بالائی داده غیر ضروری در حال جابجائی است. تمامی گره ها، عضوء یک Broadcast domain و collision domain یکسانی می باشند، بنابراین تمامی آنان هر نوع collision و یا Broadcast را که اتفاق خواهد افتاد ، می شنوند.

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



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

تعداد اندکی از هاب ها دارای یک اتصال خاص از نوع BNC بوده که می توان از آن به منظور اتصال یک کابل کواکسیال، استفاده نمود. پس از اتصال فوق، LED مربوط به اتصال BNC روی هاب روشن می گردد.

سوئیچ

شبکه از مجموعه ای کامپیوتر (گره) که توسط یک محیط انتقال (کابلی بدون کابل) بیکدیگر متصل می گردند، تشکیل شده است. در شبکه از تجهیزات خاصی نظیر هاب و روتر نیز استفاده می گردد. سوئیچ یکی از عناصر اصلی و مهم در شبکه های کامپیوتری است. با استفاده از سوئیچ، چندین کاربرقادربه ارسال اطلاعات از طریق شبکه در یک لحظه خواهند بود. سرعت ارسال اطلاعات هر یک از کاربران بر سرعت دستیابی سایر کاربران شبکه تاثیر نخواهد گذاشت. سوئیچ همانند روتر که امکان ارتباط بین چندین شبکه را فراهم می نماید، امکان ارتباط گره های متفاوت (معمولا" کامپیوتر) یک شبکه را مستقیما" با یکدیگر فراهم می نماید. شبکه ها و سوئیچ ها دارای انواع متفاوتی می باشند.. سوئیچ هائی که برای هر یک از اتصالات موجود در یک شبکه داخلی استفاده می گردند، سوئیچ های LAN نامیده می شوند. این نوع سوئیچ ها مجموعه ای از ارتباطات شبکه را بین **صرفا" دو دستگاه** که قصد ارتباط با یکدیگر را دارند، در زمان مورد نظر ایجاد می نماید.

مبانی شبکه

عناصر اصلی در یک شبکه کامپیوتری بشرح زیر می باشند:

- **شبکه** . شبکه شامل مجموعه ای از کامپیوترهای متصل شده (با یک روش خاص)، به منظور تبادل اطلاعات است.
- **گره** . گره ، شامل هر چیزی که به شبکه متصل می گردد، خواهد بود.(کامپیوتر، چاپگر و ...)
- **سگمنت**. سگمنت یک بخش خاص از شبکه بوده که توسط یک سوئیچ، روتر و یا Bridge از سایر بخش ها جدا شده است.
- **ستون فقرات** . کابل اصلی که تمام سگمنت ها به آن متصل می گردند. معمولا" ستون فقرات یک شبکه دارای سرعت بمراتب بیشتری نسبت به هر یک از

سگمنت های شبکه است . مثلا" ممکن است نرخ انتقال اطلاعات ستون فقرات شبکه ۱۰۰ مگابیت در ثانیه بوده در صورتی که نرخ انتقال اطلاعات هر سگمنت ۱۰ مگابیت در ثانیه باشد.

- **توپولوژی** . روشی که هر یک از گره ها به یکدیگر متصل می گردند را گویند.
- **کارت شبکه** . هر کامپیوتر از طریق یک کارت شبکه به شبکه متصل می گردد.در اکثر کامپیوترهای شخصی، کارت فوق از نوع اترنت بوده (دارای سرعت ۱۰ و یا ۱۰۰ مگابیت در ثانیه) و در یکی از اسلات های موجود روی برد اصلی سیستم، نصب خواهد شد.
- **آدرس MAC** . آدرس فیزیکی هر دستگاه (کارت شبکه) در شبکه است. آدرس فوق یک عدد شش بایتی بوده که سه بایت اول آن مشخص کننده سازنده کارت شبکه و سه بایت دوم ، شماره سریال کارت شبکه است.
- **Unicast** . ارسال اطلاعات توسط یک گره با آدرس خاص و دریافت اطلاعات توسط گره دیگر است.
- **Multicast** . یک گره، اطلاعاتی را برای یک گروه خاص (با آدرس مشخص) ارسال می دارد.دستگاههای موجود در گروه، اطلاعات ارسالی را دریافت خواهند کرد.
- **Broadcast** . یک گره اطلاعاتی را برای تمام گره های موجود در شبکه ارسال می نماید.

استفاده از سوئیچ

در اکثر شبکه های متداول ، به منظور اتصال گره ها از هاب استفاده می شود. همزمان با رشد شبکه (تعداد کاربران ، تنوع نیازها، کاربردهای جدید شبکه و ...) مشکلاتی در شبکه های فوق بوجود می آید:

- **Scalability** . در یک شبکه مبتنی بر هاب ، پهنای باند بصورت مشترک توسط کاربران استفاده می گردد. با توجه به محدود بودن پهنای باند ، همزمان با توسعه، کارآئی شبکه بشدت تحت تاثیر قرار خواهد گرفت. برنامه های کامپیوتر که امروزه به منظور اجراء بر روی محیط شبکه، طراحی می گردنند به پهنای باند مناسبی نیاز خواهند داشت . عدم تامین پهنای باند مورد نیازبرنامه ها، تاثیر منفی در عملکرد آنها را بدنبال خواهد داشت.
- **Latency** . به مدت زمانی که طول خواهد کشید تا بسته اطلاعاتی به مقصد مورد نظر خود برسد، اطلاق می گردد. با توجه به اینکه هر گره در شبکه های مبتنی بر هاب می بایست مدت زمانی را در انتظار سپری کرده (ممانعت از تصادم اطلاعات)، بموازات افزایش تعداد گره ها در شبکه، مدت زمان فوق افزایش خواهد یافت. در این نوع شبکه ها در صورتی که یکی از کاربران فایل با ظرفیت بالائی را برای کاربر دیگر ارسال نماید، تمام کاربران دیگر می بایست در انتظاز آزاد شدن محیط انتقال به منظور ارسال اطلاعات باشند. بهرحال افزایش مدت زمانی که یک بسته اطلاعاتی به مقصد خود برسد، هرگز مورد نظر کاربران یک شبکه نخواهد بود.
- **Failure Network** . در شبکه های مبتنی بر هاب، یکی از دستگاههای متصل شده به هاب قادر به ایجاد مسائل و مشکلاتی برای سایر دستگاههای موجود در شبکه خواهد بود. عامل بروز اشکال می تواند عدم تنظیم مناسب سرعت (مثلا" تنظیم سرعت یک هاب با قابلیت ۱۰ مگابیت در ثانیه به ۱۰۰ مگابیت در ثانیه) و یا ارسال بیش از حد بسته های اطلاعاتی از نوع Broadcast ، باشد.
- **Collisions** . در شبکه های مبتنی بر تکنولوژی اترنت از فرآینده خاصی با نام CSMA/CD به منظور ارتباط در شبکه استفاده می گردد. فرآیند فوق نحوه استفاده از محیط انتقال به منظور ارسال اطلاعات را قانونمند می نماید.

- در چنین شبکه هائی تا زمانیکه بر روی محیط انتقال ترافیک اطلاعاتی باشد، گره ای دیگر قادر به ارسال اطلاعات نخواهد بود. در صورتی که دو گره در یک لحظه اقدام به ارسال اطلاعات نمایند، یک تصادم اطلاعاتی ایجاد و عملا" بسته های اطلاعاتی ارسالی توسط هر یک از گره ها نیز از بین خواهند رفت. هر یک از گره های مربوطه (تصادم کننده) می بایست بمدت زمان کاملا" تصادفی در انتظار باقی مانده و پس از فراهم شدن شرایط ارسال، اقدام به ارسال اطلاعات مورد نظر خود نمایند.

هاب مسیر ارسال اطلاعات از یک گره به گره دیگر را به حداقل مقدار خود می رساند ولی عملا" شبکه را به سگمنت های گسسته تقسیم نمی نماید. سوئیچ به منظور تحقق خواسته فوق عرضه شده است. یکی از مهمترین تفاوت های موجود بین هاب و سوئیچ، تفسیر هر یک از پهنای باند است. تمام دستگاههای متصل شده به هاب، پهنای باند موجود را بین خود به اشتراک می گذارند.در صورتی که یک دستگاه متصل شده به سوئیچ، دارای تمام پهنای باند مختص خود است. مثلا" در صورتی که ده گره به هاب متصل شده باشند، (در یک شبکه ده مگابیت درثانیه) هر گره موجود در شبکه بخشی از تمام پهنای باند موجود (ده مگابیت در ثانیه) را اشغال خواهد کرد. (در صورتی که سایرگره ها نیز قصد ارتباط را داشته باشند). در سوئیچ، هریک از گره ها قادر به برقراری ارتباط با سایرگره ها با سرعت ده مگابیت در ثانیه خواهد بود.

در یک شبکه مبتنی بر سوئیچ، برای **هر گره** یک سگمنت اختصاصی ایجاد خواهد شد. سگمنت های فوق به یک سوئیچ متصل خواهند شد. در حقیقت سوئیچ امکان حمایت از چندین (در برخی حالات صدها) سگمنت اختصاصی را دارا است. با توجه به اینکه تنها دستگاه های موجود در هر سگمنت سوئیچ گروه می باشند، سوئیچ قادر به انتخاب اطلاعات، قبل از رسیدن به سایر گره ها خواهد بود. در ادامه سوئیچ، فریم های اطلاعاتی را به سگمنت مورد نظر هدایت خواهد کرد. با توجه به اینکه هر سگمنت دارای صرفا" یک گره می باشد، اطلاعات مورد نظر به مقصد مورد نظر ارسال خواهند شد.

بدین ترتیب در شبکه های مبتنی بر سوئیچ امکان چندین مبادله اطلاعاتی بصورت همزمان وجود خواهد داشت .

با استفاده از سوئیچ، شبکه های اترنت بصورت full-duplex خواهند بود. قبل از مطرح شدن سوئیچ، اترنت بصورت half-duplex بود. در چنین حالتی داده ها در هر لحظه امکان ارسال در یک جهت را دارا می باشند . در یک شبکه مبتنی بر سوئیچ، هر گره صرفا" با سوئیچ ارتباط برقرار می نماید (گره ها مستقیما" با یکدیگر ارتباط برقرار نمی نمایند). در چنین حالتی اطلاعات از گره به سوئیچ و از سوئیچ به گره مقصد بصورت همزمان منتقل می گردند.

در شبکه های مبتنی بر سوئیچ امکان استفاده از کابل های بهم تابیده و یا فیبر نوری وجود خواهد داشت . هر یک از کابل های فوق دارای کانکتورهای مربوط به خود برای ارسال و دریافت اطلاعات می باشند. با استفاده از سوئیچ، شبکه ای عاری از تصادم اطلاعاتی بوجود خواهد آمد. انتقال دو سویه اطلاعات در شبکه های مبتنی بر سوئـــیچ ، سرعت ارسال و دریافت اطلاعات افزایش می یابد.

اکثر شبکه های مبتنی بر سوئیچ بدلیل قیمت بالای سوئیچ ، صرفا" از سوئیچ به تنهائی استفاده نمی نمایند. در این نوع شبکه ها از ترکیب هاب و سوئیچ استفاده می گردد. مثلا" یک سازمان می تواند از چندین هاب به منظور اتصال کامپیوترهای موجود در هر یک از دپارتمانهای خود استفاده و در ادامه با استفاده از یک سوئیچ تمام هاب ها(مربوط به هر یک از دپارتمانها) بیکدیگر متصل می گردد.

تکنولوژی سوئیچ ها

سوئیچ ها دارای پتانسیل های لازم به منظور تغییر روش ارتباط هر یک از گره ها با یکدیگر می باشند. تفاوت سوئیچ با روتر چیست؟ سوئیچ ها معمولا" در لایه دوم (Data layer) مدل OSI فعالیت می نمایند.در لایه فوق امکان استفاده از آدرس های MAC (آدرس ها ی فیزیکی) وجود دارد. روتر در لایه سوم (Network) مدل OSI

فعالیت می نمایند. در لایه فوق از آدرس های IP ر IPX و یا Appeltalk استـــفاده می شود. (آدرس ها ی منطقی). الگوریتم استفاده شده توسط سوئیچ به منظور اتخاذ تصمیم در رابطه با مقصد یک بسته اطلاعاتی با الگوریتم استفاده شده توسط روتر، متفاوت است.

یکی از موارد اختلاف الگوریتم های سوئیچ و هاب، نحوه برخورد آنان با Broadcast است . مفهوم بسته های اطلاعاتی از نوع Broadcast در تمام شبکه ها مشابه می باشد. در چنین مواردی، دستگاهی نیاز به ارسال اطلاعات داشته ولی نمی داند که اطلاعات را برای چه کسی می بایست ارسال نماید. بدلیل عدم آگاهی و دانش نسبت به هویت دریافت کننده اطلاعات، دستگاه مورد نظر اقدام به ارسال اطلاعات بصورت broadcast می نماید. مثلا" هر زمان که کامپیوتر جدید ویا یکدستگاه به شبکه وارد می شود ، یک بسته اطلاعاتی از نوع Broadcast برای معرفی و حضور خود در شبکه ارسال می دارد. سایر گره ها قادر به افزودن کامپیوتر مورد نظر در لیست خود و برقراری ارتباط با آن خواهند بود. بنابراین بسته های اطلاعاتی از نوع Broadcast در مواردیکه یک دستگاه نیاز به معرفی خود به سایر بخش های شبکه را داشته و یا نسبت به هویت دریافت کننده اطلاعات شناخت لازم وجود نداشته باشند، استفاده می گردند.

هاب و یا سوئیچ ها قادر به ارسال بسته ای اطلاعاتی از نوع Broadcast برای سایر سگمنت های موجود در حوزه Broadcast می باشند.

روتر عملیات فوق را انجام نمی دهد. در صورتی که آدرس یکدستگاه مشخص نگردد ، روتر قادر به مسیریابی بسته اطلاعاتی مورد نظر نخواهد بود. ویژگی فوق در مواردیکه قصد جداسازی شبکه ها از یکدیگر مد نظر باشد ، بسیار ایده آل خواهد بود. ولی زمانیکه هدف مبادله اطلاعاتی بین بخش های متفاوت یک شبکه باشد، مطلوب بنظر نمی آید. سوئیچ ها با هدف برخورد
با مشکل فوق عرضه شده اند.

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

سوئیچ های مبتنی بر بسته های اطلاعاتی به منظور مسیریابی ترافیک موجود در شبکه از سه روش زیر استفاده می نمایند.

- Cut-Through
- Store-and-forward
- Fragment-free

سوئیچ های Cut-through ، بلافاصله پس از تشخیص بسته اطلاعاتی توسط سوئیچ ، آدرس MAC خوانده می شود. پس از ذخیره سازی شش بایت اطلاعات که شامل آدرس می باشند، بلافاصله عملیات ارسال بسته های اطلاعاتی به گره مقصد آغاز می گردد. (همزمان با دریافت سایر بسته های اطلاعاتی توسط سوئیچ). با توجه به عدم وجود کنترل های لازم در صورت بروز خطاء در روش فوق، سوئیچ های زیادی از روش فوق استفاده نمی نمایند.

سوئیچ های store-and-forward ، تمام بسته اطلاعاتی را در بافر مربوطه ذخیره و عملیات مربوط به بررسی خطاء (CRC) و سایر مسائل مربوطه را قبل از ارسال اطلاعات انجام خواهند داد. در صورتی که بسته اطلاعاتی دارای خطاء باشد، بسته اطلاعاتی دور انداخته خواهد شد. .در غیراینصورت، سوئیچ با استفاده از آدرس MAC ، بسته اطلاعاتی را برای گره مقصد ارسال می نماید. اغلب سوئیچ ها از ترکیب دو روش گفته شده استفاده می نمایند. در این نوع سوئیچ ها از روش cut-through استفاده شده و بمحض بروز خطاء از روش store-and-forward استفاده می نمایند. یکی دیگر از روش های مسیریابی ترافیک در سوئیچ ها که کمتر استفاده می گردد، fragment-free است. روش فوق مشابه cut-through بوده با این تفاوت که قبل از ارسال بسته اطلاعاتی ٦٤ بایت آن ذخیره می گردد.

سوئیچ های LAN دارای مدل های متفاوت از نقطه نظر طراحی فیزیکی می باشند. سه مدل رایج در حال حاضر بشرح زیر می باشند:

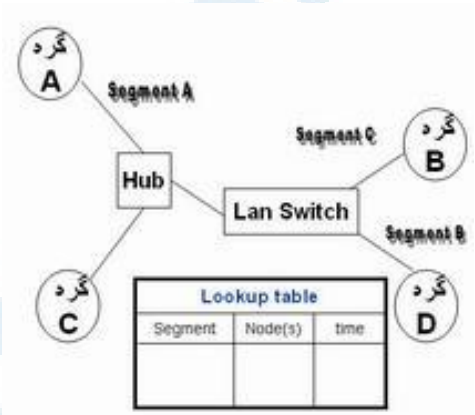
- **Shared memory** . این نوع از سوئیچ ها تمام بسته های اطلاعاتی اولیه در بافر مربوط به خود را ذخیره می نمایند. بافر فوق بصورت مشترک توسط تمام پورت های سوئیچ (اتصالات ورودی و خروجی) استفاده می گردد. در ادامه اطلاعات مورد نظر بکمک پورت مربوطه برای گره مقصد ارسال خواهند شد.
- **Matrix**. این نوع از سوئیچ ها دارای یک شبکه(تور) داخلی ماتریس مانند بوده که پورت های ورودی و خروجی همدیگر را قطع می نمایند. زمانیکه یک بسته اطلاعاتی بر روی پورت ورودی تشخیص داده شد، آدرس MAC آن با جدول lookup مقایسه تا پورت مورد نظر خروجی آن مشخص گردد. در ادامه سوئیچ یک ارتباط را از طریق شبکه و در محلی که پورت ها همدیگر را قطع می کنند، برقرار می گردد.

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

Transparent Bridging

اکثر سوئیچ های LAN مبتنی بر اترنت از سیستم ی با نام transparent bridging برای ایجاد جداول آدرس lookup استفاده می نمایند. تکنولوژی فوق امکان یادگیری هر چیزی در رابطه با محل گره های موجود در شبکه ، بدون حمایت مدیریت شبکه را فراهم می نماید. تکنولوژی فوق داری پنج بخش متفاوت است:

- Learning
- Flooding
- Filtering
- Forwarding
- Aging



نحوه عملکرد تکنولوژی فوق بشرح زیر است:

- سوئیچ به شبکه اضافه شده و تمام سگمنت ها به پورت های سوئیچ متصل خواهند شد.
- گره A بر روی اولین سگمنت (سگمنت A)، اطلاعاتی را برای کامپیوتر دیـــگر (گره B) در سگمنت دیگر (سگمنت C) ارسال می دارد.

- سوئیچ اولین بسته اطلاعاتی را از گره A دریافت می نماید. آدرس MAC آن خوانده شده و آن را در جدول Lookup سگمنت A ذخیره می نماید. بدین ترتیب سوئیچ از نحوه یافتن گره A آگاهی پیدا کرده و اگر در آینده گره ای قصد ارسال اطلاعات برای گره A را داشته باشد، سوئیچ در رابطه با آدرس آن مشکلی نخواهد داشت . فرآیند فوق را Learning می گویند.
- با توجه به اینکه سوئیچ دانشی نسبت به محل گره B ندارد، یک بسته اطلاعاتی را برای تمام سگمنت های موجود در شبکه (بجز سگمنت A که اخیرا" یکی از گره های موجود در آن اقدام به ارسال اطلاعات نموده است.) فرآیند ارسال یک بسته اطلاعاتی توسط سوئیچ، به منظور یافتن یک گره خاص برای تمام سگمنت ها ، Flooding نامیده می شود.
- گره B بسته اطلاعاتی را دریافت و یک بسته اطلاعاتی را به عنوان Acknowledgement برای گره A ارسال خواهد کرد.
- بسته اطلاعاتی ارسالی توسط گره B به سوئیچ می رسد. در این زمان، سوئیچ قادر به ذخیره کردن آدرس MAC گره B در جدول Lookup سگمنت C می باشد. با توجه به اینکه سوئیچ از آدرس گره A آگاهی دارد، بسته اطلاعاتی را مستقیما" برای آن ارسال خواهد کرد. گره A در سگمنتی متفاوت نسبت به گره B قرار دارد، بنابراین سوئیچ می بایست به منظور ارسال بسته اطلاعاتی دو سگمنت را به یکدیگر متصل نمائید. فرآیند فوق Forwarding نامیده می شود.
- در ادامه بسته اطلاعاتی بعدی از گره A به منظور ارسال برای گره B به سوئیچ می رسد، با توجه به اینکه سوئیچ از آدرس گره B آگاهی دارد، بسته اطلاعاتی فوق مستقیما" برای گره B ارسال خواهد شد.
- گره C اطلاعاتی را از طریق سوئیچ برای گره A ارسال می دارد. سوئیچ آدرس MAC گره C را در جدول Lookup سگمنت A ذخیره می نماید، سوئیچ آدرس گره A را دانسته و مشخص می گردد که دو گره A و C در یک سگمنت

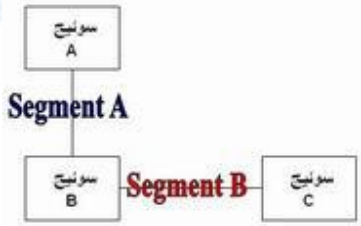
قرار دارند. بنابراین نیازی به ارتباط سگمنت A با سگمنت دیگر به منظور ارسال اطلاعات گره C نخواهد بود. بدین ترتیب سوئیچ از حرکت بسته های اطلاعاتی بین گره های موجود در یک سگمنت ممانعت می نماید. فرآیند فوق را Filtering می گویند.

- Learning و Flooding ادامه یافته و بموازات آن سوئیچ، آدرس های MAC مربوط به گره ها را در جداول Lookup ذخیره می نماید. اکثر سوئیچ ها دارای حافظه کافی به منظور ذخیره سازی جداول Lookup می باشند. به منظور بهینه سازی حافظه فوق ، اطلاعات قدیمی تر از جداول فوق حذف تا فرآیند جستجو و یافتن آدرس ها در یک زمان معقول و سریعتر انجام پذیرد. بذین منظور سوئیچ ها از روشی با نام aging استفاده می نمایند. زمانیکه یک Entry برای یک گره در جدول Lookup اضافه می گردد ، به آن یک زمان خاص نسبت داده می شود. هر زمان که بسته ای اطلاعاتی از طریق یک گره دریافت می گردد، زمان مورد نظر بهنگام می گردد. سوئیچ دارای یک یک تایمر قابل پیکربندی بوده که با عث می شود، Entry های موجود در جدول Lookup که مدت زمان خاصی از آنها استفاده نشده و یا به آنها مراجعه ای نشده است، حذف گردند . با حذف Entry های غیرضروری، حافظه قابل استفاده برای سایر Entry ها بیشتر می گردد.

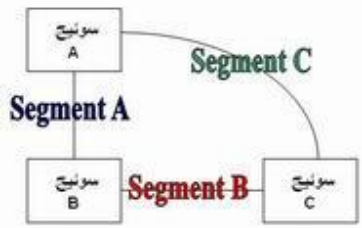
در مثال فوق، دو گره سگمنت A را به اشتراک گذاشته و سگمنت های A و D بصورت مستقل می باشند. در شبکه های ایده آل مبتنی بر سوئیچ، هرگره دارای سگمنت اختصاصی مربوط بخود است. بدین ترتیب امکان تصادم حذف و نیازی به عملیات Filtering نخواهد بود.

فراوانی و آشفتگی انتشار

در شبکه های با توپولوژی ستاره (Star) و یا ترکیب Bus و وStar یکی از عناصر اصلی شبکه که می تواند باعث از کار افتادن شبکه گردد، هاب و یا سوئیچ است. فرض کنید شبکه ای با ساختار زیر را داشته باشیم:

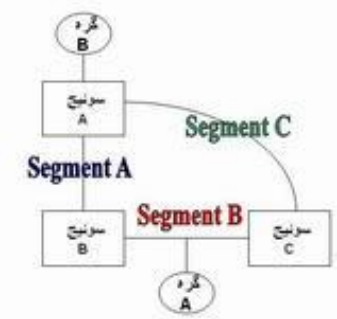


در مثال فوق، در صورتی که سوئیچ A و یا C با مشکل مواجه گردند، تمام گره های متصل به هر یک از سوئیچ های فوق نیز تحت تاثیر اشکال فوق قرار خواهند گرفت. گره های متصل به سوئیچ دیگر (B) کماکن قادر به ارائه خدمات خود خواهد بود. در صورتی که سوئیچ C با اشکال مواجه گردد، تمام شبکه از کار خواهد افتاد. در صورت اضافه کردن سگمنت دیگر برای ارتباط سوئیچ A و C چه اتفاقی خواهد افتاد.



در حالت فوق ، در صورتی که یکی از سوئیچ ها با اشکال مواجه گردد ، شبکه کماکن قادر به ارائه خدمات خودخواهد بود. با افزدون سگمنت فوق، شبکه از حالت وابستگی به یک نقطه خارج و یک نوع " فراوانی" ایجاد شده است.

با حل مشکل وابستگی عملیاتی شبکه به یک نقطه، مشکل دیگری بوجود می آید. همانگونه که قبلا" اشاره گردید، سوئیچ ها بصورت هوشمندانه ازآدرس و محل هر یک از گره های موجود در شبکه آگاه می گردند. با توجه به شرایط ایجاد شده، تمام سوئیچ ها در یک Loop به یکدیگر متصل می گردند. در چنین حالتی یک بسته اطلاعاتی ارسال شده توسط یک گره، ممکن است توسط سوئیچی از سگمنت دیگر آمده باشد.



مثلا" فرض نمائید که گره B به سوئیچ A متصل و قصد ارسال اطلاعات برای گره B موجود در سگمنت B را داشته باشد. سوئیچ A شناختی نسبت به گره A ندارد، بنابراین بسته اطلاعاتی را برای سایر گره های موجود در سگمنت های دیگر ارسال خواهد کرد. بسته اطلاعاتی مورد نظر از طریق سگمنت های A و یا C برای سایر سوئیچ ها (B و یا C) حرکت خواهد کرد. سوئیچ B، گره B را به جدول Lookup خود اضـــــافه می نماید. (برای سگمنت A). سوئیچ C آدرس گره B را به منظور پشتیبانی سگمنت C در جدول Lookup خود ذخیره خواهد کرد. با توجه به اینکه هیچکدام از سوئیچ ها تاکنون شناختی نسبت به آدرس گره A بدست نیاورده اند ، سگمنت B برای پیدا کردن گره A مورد بررسی قرار خواهد گرفت . هر سوئیچ بسته اطلاعاتی ارسال شده را دریافت و مجددا" آن را برای سایر سگمنت ها ارسال خواهد کرد. (چون هیچکدام هنوز دانشی نسبت به محل گره A را کسب نکرده اند) سوئیچ A بسته اطلاعاتی ارسالی توسط هر یک از سوئیچ ها را دریافت و مجددا" آن را برای سایر سگمنت ها ارسال می نماید. در جنین شرایطی یک نوع " آشفتگی انتشار " ایجاد شده است . شرایط فوق باعث ایجاد مشکل ترافیکی در شبکه خواهد شد. به منظور حل مشکل فوق از تکنولوژی با نام Spanning trees استفاده می شود.

Spanning tress

به منظوری پیشگیری از مسئله " آشفتگی انتشار" و سایر اثرات جانبی در رابطه با Looping شرکت DEC پروتکلی با نام (Spanning-tree Protocol(STP را ایجاد نموده است . پروتکل فوق با مشخصه d۸۰۲،۱ توسط موسسه IEEE استاندارد

شده است. tree Spanning از الگوریتم STA(Spanning-tree algoritm) استفاده می نماید. الگوریتم فوق بررسی خواهد کرد آیا یک سوئیچ دارای بیش از یک مسیر برای دستیابی به یک گره خاص است. در صورت وجود مسیرهای متعدد، بهترین مسیر نسبت به سایر مسیرها کدام است؟ نحوه عملیات STP بشرح زیر است:

- به هر سوئیچ ، مجموعه ای از مشخصه ها (ID) نسبت داده می شود. یکی از مشخصه ها برای سوئیچ و سایر مشخصه ها برای هر یک از پورت ها استفاده می گردد. مشخصه سوئیچ، Bridge ID(BID) نامیده شده و دارای هشت بایت است. دو بایت به منظور مشخص نمودن اولویت و شش بایت برای مشخص کردن آدرس MAC استفاده می گردد. مشخصه پورت ها، شانزده بیتی است . شش بیت به منظور تنظیمات مربوط به اولویت و ده بیت دیگر برای اختصاص یک شماره برا ی پورت مورد نظر است.
- برای هر مسیر یک Path Cost محاسبه می گردد. نحوه محاسبه پارامتر فوق بر اساس استانداردهای ارائه شده توسط موسسه IEEE است. به منظور محاسبه مقادر فوق، ۱،۰۰۰ مگابیت در ثانیه (یک گیگابیت در ثانیه) را بر پهنای باند سگمنت متصل شده به پورت ، تقسیم می نمایند. بنابراین یک اتصال ۱۰ مگابیت در ثانیه ، دارای Cost به میزان ۱۰۰ است (۱،۰۰۰ تفسیم بر ۱۰). به منظور هماهنگ شدن با افزایش سرعت شبکه های کامپیوتری استاندارد Cost نیز اصلاح می گردد. جدول زیر مقادیر جدید STP Cost را نشان می دهد. (مقدار cost Path می تواند یک مقدار دلخواه بوده که توسط مدیریت شبکه تعریف و مشخص می گردد)

STP Cost Value	Bandwidth
250	4 Mbps
100	10 Mbps
62	16 Mbps

45 Mbps	39
100 Mbps	19
155 Mbps	14
622 Mbps	6
1 Gbps	4
10 Gbps	2

- هر سوئیچ فرآیندی را به منظور انتخاب مسیرهای شبکه که می بایست توسط هر یک از سگمنت ها استفاده گردد، آغاز می نمایند. اطلاعات فوق توسط سایر سوئیچ ها و با استفاده از یک پروتکل خاص با نام BPUD(Bridge protocol data units) به اشتراک گذاشته می شود. ساختار یک BPUD بشرح زیر است :

- Root BID . پارامتر فوق BID مربوط به Root Bridge جاری را مشخص می کند.

- Path Cost to Bridge . مسافت root bridge را مشخص می نماید. مثلاً" در صورتی که داده از طریق طی نمودن سه سگمنت با سرعتی معادل ۱۰۰ مگابیت در ثانیه برای رسیدن به Root bridge باشد ، مقدار cost بصورت (۱۹+۱۹+۰=۳۸) بدست می آید. سگمنتی که به Root Bridge متصل است دارای Cost معادل صفر است.

- Sender BID . مشخصه BID سوئیچ ارسال کننده BPDU را مشخص می کند.

- Port ID . پورت ارسال کننده BPDU مربوط به سوئیچ را مشخص می نماید.

تمام سوئیچ ها به منظور مشخص نمودن بهترین مسیر بین سگمنت های متفاوت، بصورت پیوسته برای یکدیگر BPDUارسال می نمایند. زمانیکه سوئیچی یک BPDU

را (از سوئیچ دیگر) دریافت می دارد که مناسبتر از آن چیزی است که خود برای ارسال اطلاعات در همان سگمنت استفاده کرده است، BPDU خود را متوقف (به سایر سگمنت ها اراسال نمی نماید) و از BPDU سایر سوئیچ ها به منظور دستیابی به سگمنت ها استفاده خواهد کرد.

- یک Root bridge بر اساس فرآیندهای BPDU بین سوئیچ ها، انتخاب می گردد. در ابتدا هر سوئیچ خود را به عنوان Root در نظر می گیرد. زمانیکه یک سوئیچ برای اولین بار به شبکه متصل می گردد، یک BPDU را بهمراه BID خود که به عنوان Root BID است، ارسال می نماید. زمانیکه سایر سوئیچ ها BPDU را دریافت می دارند، آن را با BID مربوطه ای که به عنوان Root BID ذخیره نموده اند، مقایسه می نمایند. در صورتی که Root BID جدید دارای یک مقدار کمتر باشد، تمام سوئیچ ها آن را با آنچیزی که قبلا" ذخیره کرده اند، جایگزین می نمایند. در صورتی که Root BID ذخیره شده دارای مقدار کمتری باشد، یک BPDU برای سوئیچ جدید بهمراه BID مربوط به **Root BID** ارسال می گردد. زمانیکه سوئیچ جدید BPDU را دریافت می دارد، از Root بودن خود صرفنظر و مقدار ارسالی را به عنوان Root BID در جدول مربوط به خود ذخیره خواهد کرد.
- با توجه به محل Root Bridge، سایر سوئیچ ها مشخص خواهند کرد که کدامیک از پورت های آنها دارای کوتاهترین مسیر به Bridge Root است. پورت های فوق، Root Ports نامیده شده و هر سوئیچ می بایست دارای یک نمونه باشد.
- سوئیچ ها مشخص خواهند کرد که چه کسی دارای پورت های designated است . پورت فوق ، اتصالی است که توسط آن بسته های اطلاعاتی برای یک سگمنت خاص ارسال و یا از آن دریافت خواهند شد. با داشتن صرفا" یک نمونه از پورت های فوق ، تمام مشکلات مربوط به Looping برطرف خواهد شد.

- پورت های designated بر اساس کوتاهترتن مسیر بین یک سگمنت تا root bridge انتخاب می گردند. با توجه به اینکه Root bridge دارای مقدار صفر بـــرای cost path است، هر پورت آن بمنـــزله یک پورت designated است. (مشروط به اتصال پورت مورد نظر به سسگمنت) برای سایر سوئیچ ها، Path Cost برای یک سگمنت بررسی می گردد. در صورتی که پورتی دارای پایین ترین path cost باشد، پورت فوق بمنزله پورت designated سگمنت مورد نظر خواهد بود. در صورتی که دو و یا بیش از دو پورت دارای مقادیر یکسان cost path باشند، سوئیچ با مقادر کمتر BID اتخاب می گردد.
- پس از انتخاب پورت designatedبرای سگمنت شبکه، سایر پورت های متصل شده به سگمنت مورد نظر به عنوان non -designated port در نظر گرفته خواهند شد. بنابراین با استفاده از پورت های designated می توان به یک سگمنت متصل گردید.
- هر سوئیچ دارای جدول BPDU مربوط به خود بوده که بصورت خودکار بهنگام خواهد شد. بدین ترتیب شبکه بصورت یک spanning tree بوده که roor bridge که بمنزله ریشه و سایر سوئیچ ها بمنزله برگ خواهند بود. هر سوئیچ با استفاده از Root Ports قادر به ارتباط با root bridge بوده و با استفاده از پورت های designated قادر به ارتباط با هر سگمنت خواهد بود.

روترها و سوئیچینگ لایه سوم

همانگونه که قبلا" اشاره گردید، اکثر سوئیچ ها در لایه دوم مدل OSI فعالیت می نمایند (Data Layer). اخیرا" برخی از تولیدکنندگان سوییچ، مدلی را عرضه نموده اند که قادر به فعالیت در لایه سوم مدل OSI است. (Network Layer). این نوع سوئیچ ها دارای شباهت زیادی با روتر می باشند.

زمانیکه روتر یک بسته اطلاعاتی را دریافت می نماید ، در لایه سوم بدنبال آدرس های مبداء و مقصد گشته تا مسیر مربوط به بسته اطلاعاتی را مشخص نماید. سوئیچ های استاندارد از آدرس های MAC به منظور مشخص کردن آدرس مبداء و مقصد استفاده می نمایند.(از طریق لایه دوم) مهمترین تفاوت بین یک روتر و یک سوئیچ لایه سوم، استفاده سوئیچ های لایه سوم از سخت افزارهای بهینه به منظور ارسال داده با سرعت مطلوب نظیر سوئیچ های لایه دوم است. نحوه تصمیم گیری آنها در رابطه با مسیریابی بسته های اطلاعاتی مشابه روتر است. در یک محیط شبکه ای LAN ، سوئیچ های لایه سوم معمولاً دارای سرعتی بیشتر از روتر می باشند. علت این امر استفاده از سخت افزارهای سوئیچینگ در این نوع سوئیچ ها است. اغلب سوئیچ های لایه سوم شرکت سیسکو، بمنزله روترهائی می باشند که بمراتب از روتر ها سریعتر بوده (با توجه به استفاده از سخت افزارهای اختصاصی سوئیچینگ) و دارای قیمت ارزانتری نسبت به روتر می باشند. نحوه matching Pattern و caching در سوئیچ های لایه سوم مشابه یک روتر است. در هر دو دستگاه از یک پروتکل روتینگ و جدول روتینگ، به منظور مشخص نمودن بهترین مسیر استفاده می گردد. سوئیچ های لایه سوم قادر به برنامه ریزی مجدد سخت افزار بصورت پویا و با استفاده از اطلاعات روتینگ لایه سوم می باشند و همین امر باعث سرعت بالای پردازش بسته های اطلاعاتی می گردد. سوئیچ های لایه سوم، از اطلاعات دریافت شده توسط پروتکل روتینگ به منظور بهنگام سازی جداول مربوط به Caching استفاده می نمایند.

همانگونه که ملاحظه گردید، در طراحی سوئیچ های LAN از تکنولوژی های متفاوتی استفاده می گردد. نوع سوئیچ استفاده شده، تاثیر مستقیم بر سرعت و کیفیت یک شبکه را بدنبال خواهد داشت.

مفهوم روتینگ

روتینگ (Routing) یکی از مهمترین ویژگی های مورد نیاز در یک شبکه به منظور ارتباط با سایر شبکه ها است. در صورتی که امکان روتینگ پروتکل ها وجود نداشته باشد ، کامپیوترها قادر به مبادله داده نخواهند بود.

تعریف

از روتینگ به منظور دریافت یک بسته اطلاعاتی (packet) از یک دستگاه و ارسال آن از طریق شبکه برای دستگاهی دیگر و بر روی شبکه ای متفاوت، استفاده می گردد. در صورتی که شبکه شما دارای روتر نباشد، امکان روتینگ داده بین شبکه شما و سایر شبکه ها وجود نخواهد داشت. یک روتر به منظور مسیریابی یک بسته اطلاعاتی، می بایست آگاهی لازم در خصوص اطلاعات زیر را داشته باشد:

- آدرس مقصد
- روترهای مجاور که با استفاده از آنان امکان اخذ اطلاعات لازم در خصوص شبکه های از راه دور، فراهم می گردد .
- مسیرهای موجود به تمامی شبکه های از راه دور
- بهترین مسیر به هر یک از شبکه های از راه دور
- نحوه نگهداری و بررسی اطلاعات روتینگ

همگرائی (Convergence)

فرآیند مورد نیاز برای تمامی روترهای موجود در یک شبکه به منظور بهنگام سازی جداول روتینگ و ایجاد یک نگرش سازگار از شبکه با استفاده ار بهترین مسیرهای موجود . در زمان انجام فرآیند فوق (همگرائی)، داده کاربر ارسال نخواهد شد.

مسیر پیش فرض (Default Route)

یک مسیر استاندارد درج شده در جدول روتینگ که به عنوان اولین گزینه در نظر گرفته می شود . هر بسته اطلاعاتی که توسط یک دستگاه ارسال می گردد در ابتدا به مسیر پیش فرض ارسال خواهد شد. در صورتی که مسیر فوق مشکل داشته باشد، یک مسیر دیگر انتخاب می گردد.

مسیر ایستا (Static Route)

یک مسیر دائم که به صورت دستی درون یک جدول روتینگ درج می گردد. مسیر فوق حتی در مواردیکه ارتباط غیر فعال است در جدول روتینگ باقی مانده و صرفا" به صورت دستی حذف می گردد.

مسیر پویا (Dynamic Route)

یک مسیر که به صورت پویا (اتوماتیک) و متناسب با تغییرات شبکه ، بهنگام می گردد. مسیرهای پویا نقطه مقابل مسیرهای ایستا می باشند.

پروتکل های روتینگ

پروتکل های روتینگ به منظور استفاده در روترها، ایجاد شده اند پروتکل های فوق، بدین منظور طراحی شده اند که امکان مبادله اطلاعات جداول روتینگ بین روترها را فراهم نماید. تاکنون پروتکل های متفاوتی به منظور استفاده در شبکه هائی با ابعاد گوناگون ، طراحی و پیاده سازی شده است.

دو نوع عمده روتینگ : پویا و ایستا

روتر، با استفاده از روترهای مجاور (همسایه) و یا توسط مدیر شبکه، آگاهی لازم در خصوص شبکه های راه دور را پیدا می نماید. روتر در ادامه، یک جدول روتینگ را ایجاد که مسئولیت آن تشریح نحوه یافتن شبکه های راه دور است. در صورتی که شبکه مستقیما" متصل شده باشد، روتر در خصوص شبکه، مشکل خاصی نخواهد داشت. در صورتی که شبکه ها به یکدیگر متصل نمی باشند، روتر می بایست آگاهی لازم در خصوص شبکه های راه دور را پیدا نماید. در این رابطه از روتینگ ایستا (درج دستی مسیرها در جدول روتینگ توسط مدیر شبکه) و یا روتینگ پویا (درج اتوماتیک مسیرها در جدول روتینگ با استفاده از پروتکل های روتینگ)، استفاده می گردد.

روترها در ادامه اقدام به بهنگام سازی اطلاعات خود در ارتباط با تمامی شبکه هائی می نمایند که نسبت به آنان آگاهی لازم را پیدا نموده اند. در صورتی که تغییری ایجاد گردد (مثلا" یک روتر با مشکل مواجه شده و عملا" قادر به سرویس دهی نباشد)، پروتکل های روتینگ پویا، به صورت اتوماتیک به تمامی روترها این موضوع را اطلاع خواهند داد. در صورت استفاده از روتینگ ایستا، می بایست مدیر شبکه تغییرات لازم را در تمامی روترها ، اعمال نماید (عدم استفاده از پروتکل های روتینگ).

در روتینگ پویا از پروتکل های روتینگ به منظور نیل به اهداف زیر استفاده می گردد.

- تشخیص و نگهداری پویای روترها
- محاسبه مسیرها
- توزیع اطلاعات بهنگام شده روتینگ برای سایر روترها
- حصول توافق با سایر روترها در خصوص توپولوژی شبکه

در صورت برنامه ریزی ایستای روترها، امکان یافتن روترها و یا ارسال اطلاعات برای سایر روترها وجود نخواهد داشت. آنان داده مورد نظر را بر روی روترهائی که توسط مدیر شبکه تعریف شده است، ارسال می نمایند.

پروتکل های روتینگ پویا

در این رابطه از سه نوع(گروه) پروتکل روتینگ پویا استفاده می گردد. تفاوت عمده بین آنان، روش استفاده شده به منظور یافتن روترها و محاسبات لازم در خصوص مسیریابی آنان است.

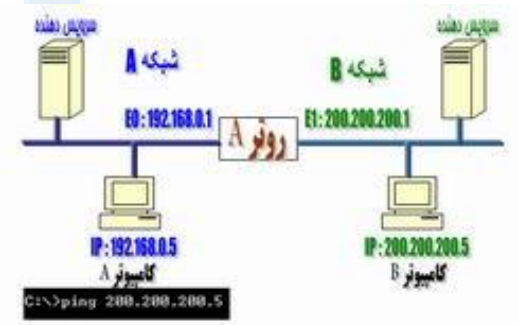
- **Distance Vector** : این نوع روترها بهترین مسیر را از طریق اطلاعات ارسال شده توسط سایر روترهای مجاور، محاسبه می نمایند.
- **Link state** : این نوع روترها هر یک دارای نسخه ای از تمامی مپ شبکه بوده و بهترین مسیر را با استفاده از آن محاسبه می نمایند.
- **Hybrid** : پروتکل های روتینگ Hybrid حد فاصل بین پروتکل های روتینگ Link state و Distance Vector می باشند.

فرآیند روتینگ

روتینگ (Routing) یکی از مهمترین پتانسیل های مورد نیاز در یک شبکه به منظور ارتباط با سایر شبکه ها است. در صورتی که امکان روتینگ پروتکل ها وجود نداشته باشد، کامپیوترها قادر به مبادله داده نخواهند بود. بسیاری از علاقه مندانی که جدیدا" به دنیای گسترده شبکه های کامپیوتری پیوسته اند، فکر می کنند که به منظور ارتباط با یک ماشین صرفا" به آدرس IP آن نیاز است. با مطالعه این مطلب مشخص خواهد شد که در این رابطه به اطلاعات بمراتب بیشتری نیاز می باشد. به منظور آشنائی با فرآیند روتینگ، یک نمونه مثال را مرحله به مرحله دنبال نموده تا با فرآیند روتینگ اطلاعات، بیشتر آشنا شویم.

مثال : برررسی فرآیند روتینگ در دو شبکه LAN

دو شبکه فرضی A و B از طریق یک روتر (روتر A) که دارای دو اینترفیس E۰ و E۱ می باشد ، به یکدیگر متصل شده اند. اینترفیس های فوق ، مشابه اینترفیس های موجود بر روی کارت های شبکه بوده که درون روتر تعبیه شده اند (RJ-45). کامپیـــوتر A (موجود بر روی شبکه A) ، قصد برقراری یک ارتباط با کامپیوتر B (مـوجود بر روی شبکه B) را دارد.



مرحله یک : کامپیوتر(میزبان)A از طریق خط دستور، فرمان ping 200.200.200.5 را تایپ می نماید.

مرحله دوم : پروتکل IP با پروتکل ARP (اقتباس شده از کلمات Address protocol Resolution) کار نموده تا مشخص گردد که بسته اطلاعاتی فوق عازم چه شبکه ای است . بدین منظور آدرس IP و Subnet Mask کامپیوتر A بررسی می گردد. با توجه به این که درخواست فوق برای یک کامپیوتر راه دور می باشـــد، می بایست بسته اطلاعاتی برای روتر (Gateway شبکه A) ارسال تا وی بتواند آن را به شبکه مورد نظر هدایت نماید (در این مورد خاص شبکه B).

مرحله سوم : کامپیوتر A به منظور ارسال بسته اطلاعاتی برای روتر، نیازمند آگاهی از آدرس سخت افزاری اینترفیس روتر است که به شبکه A متصل شده است.(منظور آدرس MAC مربوط به اینترفیس E0 است که شبکه A از طریق آن به روتر متصل شده است) . به منظور دریافت آدرس MAC، کامپیوتر A محتویات ARP cache خود را بررسی می نماید. Cache ARP، محلی از حافظه است که آدرس های MAC برای چندین ثانیه در آنجا ذخیره می گردند.

مرحله چهارم : در صورتی که آدرس MAC مربوط به اینترفیس روتر که به شبکه A متصل شده است در ARP Cache کامپیوتر A پیدا نشود ، نشاند هنده این موضوع است که مدت زمان زیادی از ارتباط وی با روتر گذشته و یا وی قادر به یافتن آدرس MAC مربوط به روتر (اینترفیسی که به شبکه A متصل شده است) نمی باشد. با توجه به وضعیت فوق ، کامپیوتر A اقدام به ارسال یک ARP broadcast می نماید. پیام ارسالی در پی یافتن پاسخی مناسب بدین سوال است که: " آدرس MAC مربوط به IP:192.168.0.1 چیست ؟". پس از ارسال پیام broadcast، روتر تشخیص می دهد که آدرس IP مربوط به وی بوده و می بایست به درخواست فوق، پاسخ دهد. بدین ترتیب، روتر با ارسال آدرس MAC مربوط به اینترفیس E0 ، پاسخ لازم را به کامپیوتر A خواهد داد.

یکی از دلایلی که در برخی مواقع دستور Ping در اولین مرتبه با Time out مواجه می شود به موضوع اشاره شده برمی گردد. در چنین مواردی مدت زمان زیادی طول خواهد کشید که یک ARP ارسال و ماشین مربوطه با ارسال آدرس MAC خود به آن پاسخ دهد (TTL:Time To Live اولین بسته اطلاعاتی Ping به سر آمده و پیام Time out را خواهیم داشت).

مرحله پنجم: روتر با ارسال آدرس IP:192.168.0.1 که به اینترفیس E0 آن نسبت داده شده است ، پاسخ مورد نظر را خواهد داد. بدین ترتیب، کامپیوتر A تمامی اطلاعات مورد نیاز به منظور ارسال یک بسته اطلاعاتی به خارج از شبکه و برای روتر را دارا می باشد. لایه شبکه به لایه DataLink که بسته اطلاعاتی را توسط Ping (یک ICMP echo request) تولید نموده است، به همراه آدرس سخت افزاری روتر، اشاره می نماید. بسته اطلاعاتی شامل آدرس های IP مبداء و مقصد به همراه ICMP echo است که در لایه شبکه مشخص شده است.

مرحله ششم : لایه DataLink مربوط به کامپیوتر A ، یک فریم را تولید که یک بسته اطلاعاتی کپسوله شده به همراه اطلاعات مورد نیاز برای ارسال بر روی شبکه محلی است (شبکه A).اطلاعات فوق، شامل آدرس سخت افزاری کامپیوترهای مبداء و مقصد (آدرس MAC) و فیلد نوع است که مسئولیت مشخص نمودن پروتکل لایه شبکه (مثلا" IPv4) و ARP را برعهده دارد. در انتهای فریم ، در بخش FCS فریم، لایه DataLink یک CRC را مستقر نموده تا ماشین دریافت کننده (روتر) قادر به تشخیص سالم بودن بسته اطلاعاتی دریافتی باشد.

مرحله هفتم : لایه DataLink کامپیوتر A ، فریم را در اختیار لایه فیزیکی قرار داده تا صفر و یک های موجود در آن به یک سیگنال دیجیتال تبدیل و بر روی محیط فیزیکی شبکه ارسال گردد .

مرحله هشتم : سیگنال ارسالی توسط اینترفیس E0 روتر برداشته شده و فریم خوانده می شود. روتر در ابتدا بخش CRC آن را بررسی و آن را با مقدار CRC اضافه شده به فریم توسط کامپیوتر A مقایسه می نماید (حصول اطمینان از عدم خرابی فریم).

مرحله نهم : در ادامه، آدرس سخت افزاری مقصد (MAC) فریم دریافتی، بررسی می گردد . با توجه به وجود یک مورد آدرس که با آن مطابقت خواهد کرد، فیلد "نوع فریم" بررسی تا نحوه برخورد روتر با بسته اطلاعاتی، مشخص گردد. IP در "فیلد نوع " بوده و روتر بسته اطلاعاتی را در اختیار پروتکل IP که بر روی روتر در حال اجراء است، قرار خواهد داد. فریم از وضعیت موجود خارج و بسته اطلاعاتی اولیه ای که توسط کامپیوتر A تولید شده است در بافر روتر ذخیره می گردد.

مرحله دهم : پروتکل IP بررسی لازم در خصوص آدرس IP مقصد را انجام داده تا مشخص گردد که آیا بسته اطلاعاتی برای روتر است.با توجه به اینکه آدرس IP: ۲۰۰،۲۰۰،۲۰۰،۵ ، می باشد، روتر با استفاده از جدول روتینگ خود تشخیص خواهد داد که آدرس فوق مربوط به شبکه ای است که از طریق اینترفیس E1 مستقیما" به روتر متصل شده است.

مرحله یازدهم : روتر، بسته اطلاعاتی را در بافر اینترفیس E1 مستقر نموده و می بایست یک فریم به منظور ارسال بسته اطلاعاتی برای کامپیوتر مقصد را تولید نماید. روتر در ابتدا ARP Cache خود را به منظور یافتن آدرس سخت افزاری مربوط به IP:200.200.200.5 ، بررسی می نماید. در صورت عدم وجود آدرس فوق در ARP cache ، روتر یک broadcast ARP را از طریق اینترفیس E1 به منظور پیدا نمودن آدرس سخت افزاری فوق، ارسال می نماید.

مرحله دوازدهم : کامپیوتر B با ارائه یک ARP Reply پاسخ لازم در خصوص آدرس سخت افزاری کارت شبکه مربوط به خود را خواهد داد . بدین ترتیب، اینترفیس E1 روتر تمامی اطلاعات لازم به منظور ارسال بسته اطلاعاتی به مقصد نهائی را دارا می باشد.

مرحله سیزدهم : فریم تولید شده توسط اینترفیس E1 روتر دارای آدرس سخت افزاری مبداء مربوط به اینترفیس E1 و آدرس سخت افزاری مقصد مربوط به کارت شبکه کامپیوتر B می باشد.با این که آدرس های سخت افزاری مبداء و مقصد فریم در هر یک از اینترفیس های روتر تغییر می نماید ، آدرس IP کامپیوترهای مبداء و مقصد هرگز تغییر پیدا نمی نماید (بسته اطلاعاتی هرگز تغییر نکرده و صرفا" فریم تغییر می نماید).

مرحله چهاردهم : کامپیوتر B ، فریم را دریافت و بررسی لازم در خصوص CRC را انجام می دهد. در صورتی که ماحصل بررسی انجام شده موفقیت آمیز نباشد، فریم دورانداخته می شود. در ادامه، آدرس IP مقصد بررسی می گردد. با توجه به این که آدرس مقصد با پیکربندی IP انجام شده بر روی کامپیوتر B ، مطابقت می نماید، فیلد پروتکل بسته اطلاعاتی بررسی تا اهداف بسته اطلاعاتی مشخص گردد.

مرحله پانزدهم : با توجه به این که بسته اطلاعاتی یک درخواست ICMP echo است، کامپیوتر B یک ICMP echo-reply جدید را که شامل آدرس IP مبداء (کامپیوتر B) و آدرس IP مقصد مربوط به کامپیوتر A می باشد را ایجاد می نماید. فرآیند فوق، مجددا" و در جهت معکوس تکرار می گردد. در این مرحله، آدرس سخت افزاری هر یک از دستگاه های موجود درطول مسیر شناخته شده بوده و هر دستگاه صرفا" نیازمند بررسی ARP cache مربوط به خود به منظور تشخیص آدرس سخت افزاری هر یک از اینترفیس ها می باشد (آدرس MAC).

روتر

اینترنت یکی از شاهکارهای بشریت در زمینه ارتباطات است. با ایجاد زیر ساخت مناسب ارتباطی، کاربران موجود در اقصی نقاط دنیا قادر به ارسال نامه های الکترونیکی، مشاهده صفحات وب، ارسال و دریافت فایل های اطلاعاتی در کمتر از چند ثانیه می باشند. شبکه ارتباطی موجود با بکارگیری انواع تجهیزات مخابراتی، سخت افزاری و نرم افزاری، زیر ساخت مناسب ارتباطی را برای عموم کاربران اینترنت فراهم آورده است. یکی از عناصر اصلی و مهم که شاید اغلب کاربران اینترنت آن را تاکنون مشاهده ننموده اند، روتر است. روترها کامپیوترهای خاصی هستند که پیام های اطلاعاتی کاربران را با استفاده از هزاران مسیر موجود به مقاصد مورد نظر هدایت می نمایند.

نحوه ارسال پیام

برای شناخت عملکرد روترها در اینترنت با یک مثال ساده شروع می نمائیم. زمانیکه برای یکی از دوستان خود، یک E-mail را ارسال می دارید ، پیام فوق به چه صورت توسط دوست شما دریافت می گردد ؟ نحوه مسیر یابی پیام فوق به چه صورت انجام می گیرد که فقط کامپیوتر دوست شما در میان میلیون ها کامپیوتر موجود در دنیا، آن را دریافت خواهد کرد.؟ اکثر عملیات مربوط به ارسال یک پیام توسط کامپیوتر فرستنده و دریافت آن توسط کامپیوتر گیرنده، توسط روتر انجام می گیرد.روترها دستگاههای خاصی می باشند که امکان حرکت پیام ها در طول شبکه را فراهم می نمایند.

به منظور آگاهی از عملکرد روتر، سازمانی را در نظر بگیرید که دارای یک شبکه داخلی و اختصاصی خود است. کارکنان سازمان فوق هر یک با توجه به نوع کار خود از شبکه استفاده می نمایند. در سازمان فوق تعدادی گرافیست کامپیوتری مشغول بکار هستند که بکمک کامپیوتر طرح های مورد نظر را طراحی می نمایند. زمانیکه یک

گرافیست فایلی را از طریق شبکه برای همکار خود ارسال می دارد، بدلیل حجم بالای فایل ارسالی، اکثر ظرفیت شبکه اشغال و بدنبال آن برای سایر کاربران ، شبکه کند خواهد شد. علت فوق (تاثیر عملکرد یک کاربر بر تمام عملکرد شبکه برای سایر کاربران) به ماهیت شبکه های اترنت برمی گردد. در شبکه های فوق هر بسته اطلاعاتی که توسط کاربری ارسال می گردد ، برای تمام کامپیوترهای موجود در شبکه نیز ارسال خواهد شد. هر کامپیوتر آدرس بسته اطلاعاتی دریافت شده را به منظور آگاهی از مقصد بسته اطلاعاتی بررسی خواهد کرد. رویکرد فوق در رفتار شبکه های اترنت ، طراحی و پیاده سازی آنان را ساده می نماید ولی همزمان با گسترش شبکه و افزایش عملیات مورد انتظار ، کارآئی شبکه کاهش پیدا خواهد کرد. سازمان مورد نظر (در مثال فوق) برای حل مشکل فوق تصمیم به ایجاد دو شبکه مجزا می گیرد. یک شبکه برای گرافیست ها ایجاد و شبکه دوم برای سایرکاربران سازمان در نظرگرفته می شود. به منظورارتباط دو شبکه فوق بیکدیگر و اینترنت از یکدستگاه روتر استفاده می گردد.

روتر، تنها دستگاه موجود در شبکه است که تمام پیامهای ارسالی توسط کامپیوترهای موجود در شبکه های سازمان، را مشاهده می نماید. زمانیکه یک گرافیست، فایلی با ظرفیت بالا را برای گرافیست دیگری ارسال می دارد، روتر آدرس دریافت کننده فایل را بررسی و با توجه به اینکه فایل مورد نظر مربوط به شبکه گرافیست ها در سازمان است، اطلاعات را بسمت شبکه فوق هدایت خواهد کرد. در صورتی که یک گرافیست اطلاعاتی را برای یکی از پرسنل شاغل در بخش مالی سازمان ارسال دارد، روتر با بررسی آدرس مقصد بسته اطلاعاتی به این نکته پی خواهد برد که پیام فوق را می بایست به شبکه دیگر انتقال دهد. بدین ترتیب روتر قادر به مسیریابی صحیح یک بسته اطلاعاتی و هدایت آن به شبکه مورد نظر شده است.

یکی از ابزارهائی که روتر از آن برای تعیین مقصد یک بسته اطلاعاتی استفاده می نماید، " **جدول پیکربندی** " است. جدول فوق شامل مجموعه اطلاعاتی بشرح ذیل است:

- اطلاعاتی در رابطه با نحوه هدایت اتصالات به آدرس های مورد نظر
- اولویت های تعریف شده برای هر اتصال
- قوانین مربوط به تبین ترافیک در حالت طبیعی وشرایط خاص

جدول فوق می تواند ساده ویا شامل صدها خط برنامه در یک روترهای کوچک باشد. در روترهای بزرگ جدول فوق پیچیده تر بوده بگونه ای که قادر به عملیات مسیریابی در اینترنت باشند. یک روتر دارای دو وظیفه اصلی است:

- تضمین عدم ارسال اطلاعات به محلی که به آنها نیاز نیست
- تضمین ارسال اطلاعات به مقصد صحیح

با توجه به وظایف اساسی فوق، مناسبترین محل استفاده از یک روتر، اتصال دو شبکه است . با اتصال دو شبکه توسط روتر، اطلاعات موجود در یک شبکه قادر به ارسال در شبکه دیگر و بالعکس خواهند بود. در برخی موارد ترجمه های لازم با توجه به پروتکل های استفاده شده در هریک از شبکه ها، نیز توسط روتر انجام خواهد شد. روتر شبکه ها را در مقابل یکدیگر حفاظت و از ترافیک غیرضروری پیشگیری می نماید. (تاثیر ترافیک موجود در یک شبکه بر شبکه دیگر با فرض غیر لازم بودن اطلاعات حاصل از ترافیک در شبکه اول برای شبکه دوم). همزمان با گسترش شبکه، جدول پیکربندی نیز رشد و توان پردازنده روتر نیز می بایست افزایش یابد. صرفنظر از تعداد شبکه هائی که به یک روتر متصل می باشند، نوع و نحوه انجام عملیات در تمامی روترها مشابه است. اینترنت به عنوان بزرگترین شبکه کامپیوتری از هزاران شبکه کوچکتر تشکیل شده است. روترها در اتصال شبکه های کوچکتر در اینترنت دارای نقشی اساسی و ضروری می باشند.

ارسال بسته های اطلاعاتی

زمانیکه از طریق تلفن با شخصی تماسی برقرار می گردد، سیستم تلفن، یک مدار پایدار بین تماس گیرنده و شخص مورد نظر ایجاد می نماید.

مدار ایجاد شده می بایست مراحل متفاوتی را با استفاده از کابل های مسی، سوئیچ ها، فیبر های نوری، ماکروویو و ماهواره انجام دهد. تمام مراحل مورد نظر به منظور برپاسازی یک ارتباط پایدار بین تماس گیرنده و مخاطب مورد نظر در مدت زمان تماس ، ثابت خواهند بود. کیفیت خط ارتباطی مشروط به عدم بروز مشکلات فنی و غیرفنی در هر یک از تجهیزات اشاره شده، در مدت برقراری تماس ثابت خواهد بود. با بروز هر گونه اشکال نظیر خرابی یک سوئیچ و .. خط ارتباطی ایجاد شده با مشکل مواجه خواهد شد.

اطلاعات موجود در اینترنت (صفحات وب ، پیام های الکترونیکی و ...) با استفاده از سیستمی با نام Packet -switching network به حرکت در می آیند. در سیستم فوق ، داده های موجود در یک پیام و یا یک فایل به بسته های ۱۵۰۰ بایتی تقسیم می گردند. هر یک از بسته های فوق شامل اطلاعات مربوط به : آدرس فرستنده ، آدرس گیرنده، موقعیت بسته در پیام و بررسی ارسال درست اطلاعات توسط گیرنده است. هر یک از بسته های فوق را Packet می گویند. در ادامه بسته های فوق با استفاده از بهترین و مناسبترین مسیر برای مقصد ارسال خواهند شد. عملیات فوق در مقایسه با سیستم استفاده شده در تلفن پیچیده تر بنظر می آید، ولی در یک شبکه مبتنی بر داده دودلیل (مزیت) عمده برای استفاده از تکنولوژی Packet switching وجود دارد:

- شبکه قادر به تنظیم لود موجود بر روی هر یک از دستگاهها با سرعت بالا است (میلی ثانیه)
- در صورت وجود اشکال در یک دستگاه، بسته اطلاعاتی از مسیر دیگر عبور داده شده تا به مقصد برسد.

روترها که بخش اصلی شبکه اینترنت را تشکیل می دهند، قادر به " پیکربندی مجدد مسیر " بسته های اطلاعاتی می باشند. در این راستا شرایط حاکم بر خطوط نظیر تاخیر در دریافت و ارسال اطلاعات و ترافیک موجود بر روی عناصر متفاوت شبکه بصورت دائم مورد بررسی قرار خواهند گرفت. روتر دارای اندازه های متفاوت است:

- در صورتی که از امکان Internet connection sharing بین دو کامپیوتری که بر روی آنها ویندوز ۹۸ نصب شده است استفاده گردد، یکی از کامپیوترها که خط اینترنت به آن متصل شده است به عنوان یک روتر ساده رفتار می نماید. در مدل فوق روتر، عملیات ساده ای را انجام می دهد. داده مورد نظر بررسی تا مقصد آن برای یکی از دو کامپیوتر تعیین گردد.
- روترهای بزرگتر نظیر روترهائی که یک سازمان کوچک را به اینترنت متصل می نمایند ، عملیات بمراتب بیشتری را نسبت به مدل قبلی انجام می دهند. روترهای فوق از مجموعه قوانین امنیتی حاکم بر سازمان مربوطه تبعیت و بصورت ادواری سیستم امنیتی تبین شده ای را بررسی می نمایند.
- روترهای بزرگتر مشابه روترهائی که ترافیک اطلاعات را در نقط حساس ومهم اینترنت کنترل می نمایند، در هر ثانیه میلیون ها بسته اطلاعاتی را مسیریابی می نمایند.

در اغلب سازمانها و موسسات از روترهای متوسط استفاده می گردد. در این سازمانها از روتر به منظور اتصال دو شبکه استفاده می شود. شبکه داخلی سازمان از طریق روتر به شبکه اینترنت متصل می گردد. شبکه داخلی سازمان از طریق یک خط اترنت (یک اتصال ۱۰۰base-T ۹ ، خط فوق دارای نرخ انتقال ۱۰۰ مگابیت در ثانیه بوده و از کابل های بهم تابیده هشت رشته استفاده می گردد) به روتر متصل می گردد. به منظور ارتباط روتر به مرکز ارائه دهنده خدمات اینترنت (ISP) می توان از خطوط اختصاصی با سرعت های متفاوت استفاده کرد. خط اختصاصی T1 یک نمونه متداول در این زمینه بوده و دارای سرعت ۱،۵ مگابیت در ثانیه است. برخی از موسسات با توجه به حساسیت و نوع کار خود می توانند از یک خط دیگر نیز به منظور ارتباط روتر با ISP استفاده نمایند.

خط فوق بصورت Backup بوده و بمحض بروز اشکال در خط اختصاصی(مثلا" T1) می توان از خط دوم استفاده نمود. با توجه به اینکه خط فوق بصورت موقت و در مواقع اضطراری استفاده می شود ، می توان یک خط با سرعت پایین تررا استفاده کرد.

روترها علاوه بر قابلیت روتینگ بسته های اطلاعاتی از یک نقطه به نقطه دیگر، دارای امکانات مربوط به پیاده سازی سیستم امنیتی نیز می باشند. مثلا" می توان مشخص کرد که نحوه دستیابی کامپیوترهای خارج از شبکه داخلی سازمان به شبکه داخلی به چه صورت است . اکثر سازمانها و موسسات دارای یک نرم افزار و یا سخت افزار خاص فایروال به منظور اعمال سیاســـت های امنیتی می باشند. قوانـــین تعریف شده در جدول پیکربندی روتر از لحاظ امنیتی دارای صلابت بیشتری می باشند.

یکی از عملیات ادواری (تکراری) که هر روتر انجام می دهد، آگاهی از استقرار یک بسته اطلاعاتی در شبکه داخلی است. در صورتی که بسته اطلاعاتی مربوط به شبکه داخلی بوده نیازی به روت نمودن آن توسط روتر نخواهد بود. بدین به منظور از مکانیزمی با نام Subnet mask استفاده می شود. subnet مشابه یک آدرس IP بوده و اغلب بصورت ۲۵۵،۲۵۵،۲۵۵،۰ است. آدرس فوق به روتر اعلام می نماید که تمام پیام های مربوط به فرستنده و یا گیرنده که دارای یک آدرس مشترک در سه گروه اول می باشند ، مربوط به یک شبکه مشابه بوده و نیازی به ارسال آنها برای یک شبکه دیگر وجود ندارد.

مثلا" کامپیوتری با آدرس ۱۵،۵۷،۳۱،۴۰ پیامی را برای کامپیوتر با آدرس ۱۵،۵۷،۳۱،۵۲ ارسال می دارد. روتر که در جریان تمام بسته های اطلاعاتی است، سه گروه اول در آدرس های فرستنده و گیرنده را مطابقت می نماید و بسته اطلاعاتی را بر روی شبکه داخلی نگه خواهد داشت.

آگاهی از مقصد یک پیام

روتر یکی از مجموعه دستگاههائی است که در شبکه استفاده می شود. هاب، سوئیچ و روتر سیگنال هائی را ار کامپیوترها و یا شبکه ها دریافت و آنها را برای کامپیوترها و یا شبکه های دیگر ارسال می دارند. روتر تنها دستگاه موجود می باشد که در رابطه با مسیر یک بسته اطلاعاتی تصمیم گیری می نماید. به منظور انجام عملیات فوق ، روترها می بایست نسبت به دو موضوع آگاهی داشته باشند: آدرس ها و ساختار شبکه.

زمانیکه توسط یکی از دوستانتان برای شما یک کارت تبریک سال نو ارسال می گردد ، از آدرسی مطابق زیر استفاده می نماید : " تهران- خیابان ایران - کوچه شمیرانات- پلاک ۱۱۰ " آدرس فوق دارای چندین بخش بوده که به اداره پست مربوطه امکان پیدا نمودن آدرس فوق را خواهد داد. استفاده از کد پستی باعث سرعت در ارسال کارت تبریک و دریافت آن توسط شخص مورد نظر می نماید .ولی حتی در صورتی که از کد پستی هم استفاده نشود ، امکان دریافت کارت تبریک با توجه به مشخص شدن شهرستان ، خیابان ، کوچه و پلاک نیز وجود خواهد داشت.

آدرس فوق یک نوع آدرس منطقی است. آدرس فوق روشی را برای دریافت کارت تبریک ، مشخص می نماید. آدرس فوق به یک آدرس فیزیکی مرتبط خواهد شد. هر یک از دستگاههای موجود که به شبکه متصل می گردند، دارای یک آدرس فیزیکی می باشند. آدرس فوق منحصر بفرد بوده و توسط دستگاهی که به کابل شبکه متصل است، در نظر گرفته خواهد شد. مثلا" در صورتی که کامپیوتر شما دارای یک کارت شبکه (NIC) می باشد، کارت فوق دارای یک آدرس فیزیکی دائمی بوده که در یک محل خاص از حافظه ذخیره شده است . آدرس فیزیکی که آدرس MAC (Media Access Control) نیز نامیده می شود، دارای دو بخش بوده که هر یک سه بایت می باشند. اولین سه بایت، شرکت سازنده کارت شبکه را مشخص می نماید . دومین سه بایت یک شماره سریال مربوط به کارت شبکه است.

کامپیوتر می تواند دارای چندین آدرس منطقی در یک لحظه باشد. وضعیت فوق دررابطه با اشخاص نیز صدق می کند. مثلا" یک شخص می تواند دارای آدرس پستی، شماره تلفن، آدرس پست الکترونیکی و ... باشد. از طریق هر یک از آدرس های فوق امکان ارسال پیام برای شما وجود خواهد داشت. آدرس های منطقی در کامپیونر نیز مشابه سیستم فوق کار می کنند. در این راستا ممکن است از مدل های متفاوت آدرس دهی و یا پروتکل های مربوط به شبکه های متفاوت بطور همزمان استفاده گردد. در زمان اتصال به اینترنت ، شما دارای یک آدرس بوده که از پروتکل TCP/IP مشتق شده است. در صورتی که دارای یک شبکه کوچک می باشید ، ممکن است از پروتکل NetBEUI مایکروسافت استفاده می نمائید. بهرحال یک کامپیوتر می تواند دارای چندین آدرس منطقی بوده که پروتکل استفاده شده قالب آدرس فوق را مشخص خواهد کرد.

آدرس فیزیکی یک کامپیونر می بایست به یک آدرس منطقی تبدیل گردد. از آدرس منطقی در شبکه برای ارسال و دریافت اطلاعات استفاده می گردد. برای مشاهده آدرس فیزیکی کامپیوتر خود می توانید از دستور IPCONFIG (ویندوز ۲۰۰۰و XP) استفاده نماید.

پروتکل ها

اولین و مهمترین وظیفه روتر، آگاهی از محلی است که می بایست اطلاعات ارسال گردند.

اکثر روترها که یک پیام را برای شما مسیریابی می نمایند، از آدرس فیزیکی کامپیوتر شما آگاهی ندارند. روترها به منظور شناخت اکثر پروتکل های رایج ، برنامه ریزی می گردند. بدین ترتیب روترها نسبت به فورمت هر یک از مدل های آدرس دهی دارای شناخت مناسب می باشند. (تعداد بایت های موجود در هر بسته اطلاعاتی، آگاهی از نحوه ارسال درست اطلاعات به مقصد و ...) روترها به عنوان مهمترین عناصر در ایجاد ستون فقرات اینترنت مطرح می باشند. روترها در هر ثانیه میلیون ها بسته اطلاعاتی را مسیریابی می نمایند. ارسال یک بسته اطلاعاتی به مقصد مورد نظر، تنها وظیفه یک روتر نخواهد بود. روترها می بایست قادر به یافتن بهترین مسیر ممکن باشند. دریک شبکه پیشرفته هر پیام الکترونیکی به چندین بخش کوچکتر تقسیم می گردد. بخش های فوق بصورت مجزا ارسال و در مقصد مجدداً با ترکیب بخش های فوق بیکدیگر، پیام اولیه شکل واقعی خود را پیدا خواهد کرد. بخش های اطلاعاتی اشاره شده Packet نامیده شده و هر یک ازآنان می توانند از یک مسیر خاص ارسال گردند. این نوع از شبکه ها را network Packet-Switched می گویند. در شبکه های فوق یک مسیر اختصاصی بین کامپیوتر فرستنده بسته های اطلاعاتی و گیرنده ایجاد نخواهد گردید. پیام های ارسالی از طریق یکی از هزاران مسیر ممکن حرکت تا در نهایت توسط کامپیوتر گیرنده ، دریافت گردد. با توجه به ترافیک موجود در شبکه ممکن است در برخی حالات عناصر موجود در شبکه لود بالائی را داشته باشند، در چنین مواردی روترها با یکدیگر ارتباط و ترافیک شبکه را بهینه خواهند کرد. (استفاده از مسیرهای دیگر برای ارسال اطلاعات باتوجه به وجود ترافیک بالا در بخش های خاصی از شبکه)

ردیابی یک پیام

در صورتی که از سیستم عامل ویندوز استفاده می نمائید ، با استفاده از دستور Traceroute می توانید مسیر بسته های اطلاعاتی را دنبال نمائید.

ستون فقرات اینترنت

باتوجه به گستردگی اینترنت و وجود میلیون ها بسته اطلاعاتی در هر ثانیه به منظور مسیریابی، می بایست از روترهای با سرعت بالا استفاده شود. روتر سری ۱۲۰۰۰ سیسکو یکی از این نوع روترها بوده که به عنوان ستون فقرات اصلی در اینترنت استفاده می شود. تکنولوژی بکار گرفته شده در طراحی روترهای فوق مشابه سوپر کامپیوترها می باشد. (استفاده از پردازنده های با سرعت بالا بهمراه مجموعه ای از سویئچ های پر سرعت). در روتر مدل ۱۲۰۰۰ از پردازنده های ۲۰۰MHZ MIPS R5000 استفاده می شود. ۱۲۰۱۶ ، یکی از مدل های سری فوق است . مدل فوق قادر دارای توان عملیات ۳۲۰ میلیارد بیت از اطلاعات را در ثانیه را دارد. در صورتی که مدل فوق با تمام توان و ظرفیت خود نصب گردد، امکان انتقال ۶۰ میلیون بسته اطلاعاتی در هرثانیه را دارا است.

روترها با استفاده از جدول پیکربندی خود قادر به مسیریابی صحیح بسته های اطلاعاتی خواهند بود. قوانین موجود در جدول فوق سیاست مسیریابی یک بسته اطلاعاتی را تبین خواهند کرد . قبل از ارسال بسته های اطلاعاتی توسط مسیر مشخص شده ، روتر خط (مسیر) مربوطه را از از نقطه نظر کارآئی بررسی می نماید . در صورتی که مسیر فوق فاقد کارآئی لازم باشد، روتر مسیر فوق را چشم پوشی نموده و مجدداً یک مسیر دیگر را مشخص خواهد کرد. پس از اطمینان از کارآئی مسیر مشخص شده ، بسته اطلاعاتی توسط مسیر مورد نظر ارسال خواهد گردید. تمام عملیات فوق صرفاً در کسری از ثانیه انجام می گردد. در هر ثانیه، فرآیند فوق میلیون ها مرتبه تکرار خواهد شد.

آگاهی از محلی که پیام ها می بایست ارسال گردند ، مهمترین وظیفه یک روتر است. برخی از روترهای ساده، صرفاً عملیات فوق را انجام داده و برخی دیگر از روترها عملیات بمراتب بیشتر و پیچیده تری را انجام می دهند.

راه اندازی اولیه روتر

روتر یک نوع کامپیوتر خاص است که دارای عناصر مشابه یک کامپیوتر استاندارد شخصی نظیر پردازنده، حافظه، خطوط داده و اینترفیس های مختلف ورودی و خروجی است. روترها نیز همانند کامپیوترها که برای اجرای برنامه ها به یک سیستم عامل نیاز دارند، از خدمات یک سیستم عامل در ابعاد گسترده استفاده می نمایند.

فرآیند راه اندازی روتر با استقرار برنامه Bootstrap، سیستم عامل و یک فایل پیکربندی در حافظه آغاز می گردد. در صورتی که روتر نتواند یک فایل پیکربندی را پیدا نماید، Setup mode فعال و پس از اتمام عملیات در این mode ، می توان یک نسخه backup از فایل پیکربندی را در حافظه NVRAM ذخیره نمود.

هدف از اجرای روتین های راه انداز نرم افزار IOS ، راه اندازی و آغاز فعالیت های یک روتر می باشد. بدین منظور لازم است عملیات زیر توسط روتین های راه انداز انجام شود :

- حصول اطمینان از صحت عملکرد سخت افزار روتر
- یافتن و استقرار نرم افزار IOS در حافظه
- یافتن و بکارگیری فایل پیکربندی راه انداز و یا ورود به setup mode

پس از روشن کردن روتر، در اولین اقدام برنامه ای موسوم به POST (برگرفته از power-on self-test) اجراء می گردد. برنامه فوق در حافظه ROM ذخیره و مشتمل بر روتین هائی است که تمامی عناصر سخت افزاری روتر نظیر پردازنده ، حافظه و پورت های اینترفیس شبکه را بررسی و تست می نماید.

پس از حصول اطمینان از صحت عملکرد سخت افزار، فرآیند راه اندازی روتر بر اساس مراحل زیر دنبال می شود:

- **مرحله اول : اجرای برنامه bootstrap loader موجود در حافظه ROM** . برنامه فوق، مشتمل بر مجموعه ای از دستورالعمل به منظور تست سخت افزار و مقداردهی اولیه IOS برای انجام وظایف محوله می باشد.
- **مرحله دوم : یافتن محل ذخیره IOS** . فیلد بوت ریجستر پیکربندی، مکان ذخیره IOS را تعیین می نماید. در صورتی که مشخص شده باشد که می بایست IOS از طریق حافظه فلش در حافظه مستقر گردد ولی IOS در حافظه فلش موجود نباشد ، یک نسخه از IOS با امکانات محدودتر از طریق حافظه ROM در حافظه مستقر خواهد شد .
- **مرحله سوم : استقرار IOS image در حافظه** . در این مرحله IOS در حافظه مستقر می گردد. پس از استقرار IOS در حافظه و عملیاتی شدن آن، لیستی از عناصر سخت افزاری و نرم افزاری موجود بر روی نمایشگر (کامپیوتر و یا ترمینال) نمایش داده می شود.
- **مرحله چهارم : استقرار فایل پیکربندی در حافظه و اجرای دستورات آن** . در این مرحله فایل پیکربندی ذخیره شده در حافظه NVRAM ، درون حافظه اصلی قرار گرفته و دستورات آن یکی پس از دیگری اجراء می گردند.
- **مرحله پنجم : فعال شدن mode Setup** در صورتی که IOS بگونه ای تنظیم شده باشد که وی را ملزم به استقرار فایل پیکربندی از طریق یک سرویس دهنده TFTP و یا NVRAM نماید ولی در عمل فایل پیکربندی در هیچیک از مکان های اشاره شده موجود نباشد، روتین automated setup مقداردهی اولیه می گردد. در این mode امکانات و تسهیلات لازم برای نصب حداقل پیکربندی مورد نیاز در اختیار مدیریت شبکه گذاشته می شود. در setup mode ، پاسخ های پیش فرض بین علامت [] نشان داده شده و پس از فشردن کلید Enter، گزینه پیش فرض انتخاب می گردد. پس از تکمیل فرآیند پیکربندی، گزینه های زیر نمایش داده می شوند:

```
Setup mode
 [0] Go to the IOS command prompt without saving this config.
 [1] Return back to the setup without saving this config.
 [2] Save this configuration to nvram and exit.
 Enter your selection [2]:
```

چراغ های LEDs

در زمان راه اندازی روتر، هر LED موجود با توجه به رسالت خود می تواند اطلاعات مفیدی را ارائه نماید. مثلا" LED مربوط به اینترفیس ها، وضعیت هر اینترفیس را نشان خواهد داد. در صورتی که اینترفیس فعال و به درستی متصل شده باشد ولی LED آن خاموش است، ممکن است برای اینترفیس یک مشکل خاص ایجاد شده باشد.

راه اندازی سیستم و نمایش پیام ها و اطلاعات مختلف

در زمان راه اندازی روتر اطلاعات و پیام های متفاوتی بر روی نمایشگر کامپیوتر و یا ترمینال نمایش داده می شود. اطلاعات فوق با توجه به نوع اینترفیس روتر و نسخه IOS متفاوت می باشد. در ادامه به برخی از پیام ها در زمان راه اندازی روتر اشاره می گردد:

- نمایش پیام "**NVRAM invalid، possibly due to write erase**" در زمان راه اندازی روتر این موضوع را اعلام می نماید که روتر تاکنون پیکربندی نشده و یا اطلاعات موجود در حافظه NVRAM آن حذف شده است . در چنین مواردی لازم است که روتر پیکربندی شده و فایل پیکربندی در حافظه NVRAM ذخیره و در ادامه از فایل فوق استفاده گردد. تنظیمات پیش فرض برای ریجستر پیکربندی مقدار ۰X2102 می باشد که نشاندهنده ذخیره image IOS

در حافظه فلش است و می بایست از طریق حافظه فوق به درون حافظه اصلی منتقل گردد .

- **نمایش اطلاعات نرم افزاری و سخت افزاری روتر** . در زمان راه اندازی روتر، اطلاعات متفاوتی نظیر شماره نسخه برنامه های bootstrap ، IOS ، مدل روتر، نوع پردازنده، میزان حافظه، تعداد و نوع اینترفیس ها بر روی صفحه نمایشگر کامپیوتر و یا ترمینال نمایش داده می شود.

آشنائی با سیستم عامل روتر

IOS (برگرفته از Internetwork Operating System)، نرم افزاری است که از آن به منظور کنترل روتینگ و سوئیچینگ دستگاه های بین شبکه ای استفاده می گردد. آشنائی با IOS برای تمامی مدیران شبکه و به منظور مدیریت و پیکربندی دستگاه هائی نظیر روتر و یا سوئیچ الزامی است.

در این مطلب پس از معرفی اولیه IOS به بررسی برخی از ویژگی های آن خواهیم پرداخت.

IOS و ضرورت استفاده از آن

یک روتر و یا سوئیچ بدون وجود یک سیستم عامل قادر به انجام وظایف خود نمی باشند(همانند یک کامپیوتر). شرکت سیسکو، سیستم عامل Cisco IOS را برای طیف گسترده ای از محصولات شبکه ای خود طراحی و پیاده سازی نموده است. نرم افزار فوق، جزء لاینفک در معماری نرم افزار روترهای سیسکو می باشد و همچنین به عنوان سیستم عامل در سوئیچ های Catalyst ایفای وظیفه می نماید. بدون وجود یک سیستم عامل ، سخت افزار قادر به انجام هیچگونه عملیاتی نخو اهد بود . (عدم تامین شرایط لازم برای بالفعل شدن پتانسیل های سخت افزاری).

IOS ، سرویس های شبکه ای زیر را ارائه می نماید:

- عملیات روتینگ و سوئیچینگ
- دستیابی ایمن و مطمئن به منابع شبکه
- قابلیت توسعه و تغییر پیکربندی شبکه

ماهیت اینترفیس IOS

نرم افزار IOS از یک اینترفیس خط دستوری و یا CLI (برگرفته از command-line interface) استفاده می نماید. IOS یک تکنولوژی کلیدی است که از آن در

اکثر خطوط تولید محصولات شرکت سیسکو استفاده می گردد . عملکرد IOS با توجه به نوع دستگاه های بین شبکه ای متفاوت می باشد.
برای دستیابی به محیط IOS از روش های متعددی استفاده می گردد:

- **session console** : در این روش با استفاده از یک اتصال سریال با سرعت پائین، کامپیوتر و یا دستگاه ترمینال را مستقیما" به پورت کنسول روتر متصل می نمایند. (سرویس شبکه ای خاصی بر روی روتر پیکربندی نشده است)
- **ارتباط Dialup** : در این روش با استفاده از مودم و از طریق پورت کمکی (AUX) با روتر ارتباط برقرار می گردد . (سرویس شبکه ای خاصی بر روی روتر پیکربندی نشده است).
- **استفاده از telnet** : در این روش می بایست حداقل یکی از اینترفیس ها با یک آدرس IP پیکربندی گردد و terminal sessions virtual برای login و رمز عبور پیکربندی شده باشد.

برای دستیابی به بخش رابط کاربر روتر و یا سوئیچ از یک برنامه ترمینال استفاده می گردد HyperTerminal متداولترین گزینه در این رابطه می باشد.

حالات متفاوت رابط کاربر روتر

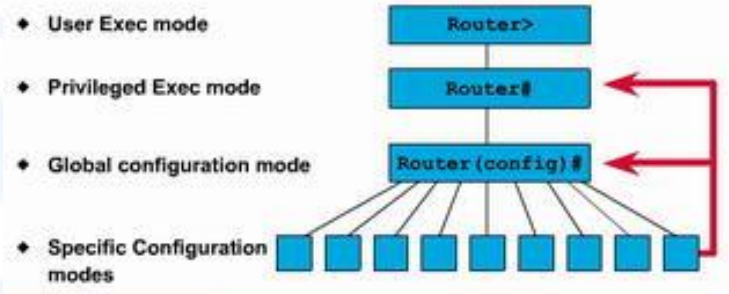
اینترفیس خط دستور و یا CLI روترهای سیسکو از یک ساختار سلسله مراتبی تبعیت می نماید. ساختار فوق کاربران را ملزم می نماید که برای انجام هر نوع عملیات خاص به یک mode بخصوص وارد شوند. مثلا" برای پیکربندی یک اینترفیس روتر، کاربر می بایست به mode پیکربندی اینترفیس و یا configuration interface mode وارد شود. هر mode پیکربندی دارای یک prompt مختص به خود می باشد که از طریق آن می توان دستورات مربوطه را تایپ و از توان عملیاتی آنان استفاده نمود.

IOS ، یک سرویس مفسر دستور با نام EXEC را ارائه می نماید. پس از درج هر دستور، EXEC صحت آن را بررسی و پس از تائید آن را اجراء می نماید. نرم افزار IOS در جهت افزایش امنیت، دو سطح متفاوت دستیابی user EXEC mode و privileged EXEC mode با ویژگی زیر را برای سرویس مفسر دستور (EXEC) در نظر می گیرد:

- **EXEC mode user** : در این mode صرفا" می توان تعداد محدودی از دستورات مانیتورینگ را اجراء نمود. به این مد view only نیز گفته شده و نمی توان دستوراتی را که باعث تغییر در پیکربندی روتر می گردند، اجراء نمود.
- **privileged EXEC mode** : در این mode می توان به تمامی دستورات روتر دسترسی داشت . برای استفاده از این mode و در جهت افزایش امنیت ، می توان روتر را بگونه ای پیکربندی نمود که کاربران را ملزم به درج نام و رمز عبور جهت دستیابی به روتر نماید. Global configuration mode و سایر حالات متفاوت پیکربندی صرفا" از طریق privileged EXEC mode قابل دستیابی می باشند.

EXEC Mode	Prompt	کاربرد
User	**Router1>**	بررسی وضعیت روتر
privileged	**Router1#**	دستیابی به حالات متفاوت پیکربندی روتر

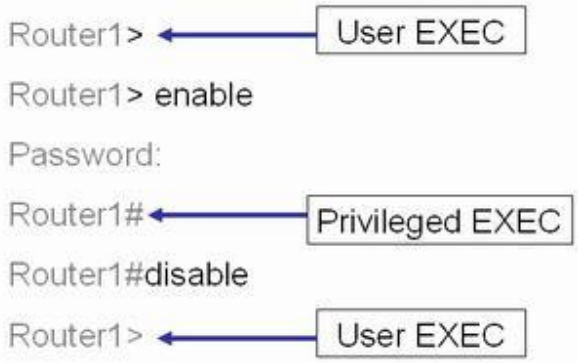
- شکل زیر حالات متفاوت پیکربندی روتر را نشان می دهد.



Configuration Mode	Prompt
Interface	Router(config-if)#
Subinterface	Router(config-subif)#
Controller	Router(config-controller)#
Map-list	Router(config-map-list)#
Map-class	Router(config-map-class)#
Line	Router(config-line)#
Router	Router(config-router)#
IPX-router	Router(config-ipx-router)#
Route-map	Router(config-route-map)#

همانگونه که در شکل فوق مشاهده می گردد ، جهت فلش قرمز رنگ به سمت Global Configuration Mode و Privileged mode است . این بدان معنی است که جهت ورود به برخی حالات خاص پیکربندی می توان از طریق Global Configuration Mode اقدام نمود و در برخی موارد دیگر این کار از طریق Privileged mode انجام می گردد .

به منظور دستیابی به privileged EXEC mode از طریق user EXEC mode ، از دستور enable استفاده می گردد . در صورتی که روتر بگونه ای پیکربندی شده است که جهت ورود به privileged EXEC mode کاربران را ملزم به درج نام و رمز عبور می نماید، می بایست در این مرحله رمز عبور را نیز وارد نمود. پس از درج صحیح رمز عبور، به EXEC mode privileged وارد شده و با درج یک علامت سوال می توان دستورات و گزینه های متعدد موجود در این mode را مشاهده نمود . شکل زیر نحوه حرکت بین user EXEC mode و privileged EXEC mode را نشان می دهد.



ویژگی نرم افزار IOS

شرکت سیسکو تاکنون نسخه های متفاوتی از نرم افزار IOS را پیاده سازی نموده است . هر image دارای ویژگی های مختص به خود می باشد .علیرغم تنوع بسیار گسترده IOS images برای دستگاه های سیسکو ، ساختار اولیه دستورات پیکربندی در آنان مشابه می باشد و در صورت کسب مهارت لازم به منظور پیکربندی و اشکال زدائی یک دستگاه خاص ، می توان از تجارب موجود در ارتباط با سایر دستگاه ها نیز استفاده نمود. اسامی در نظر گرفته شده برای هر یک از نسخه های IOS از سه بخش عمده تشکیل می گردد:

- محیطی که image بر روی آن اجراء می گردد
- ویژگی منحصربفرد image
- محل اجراء image و وضعیت فشرده بودن آن

با استفاده از Advisor Cisco Software می توان ویژگی های خاصی از IOS را انتخاب نمود. نرم افزار فوق یک ابزار محاوره ای است که پس از نمایش وضعیت موجود، امکان انتخاب گزینه هائی متناسب با واقعیت های شبکه را فراهم می نماید. یکی از مهمترین مواردی که در زمان انتخاب یک IOS image جدید می بایست به آن توجه گردد، سازگاری آن با حافظه فلش و RAM است. نسخه های جدیدتر عموما"

دارای امکانات بیشتری بوده و به حافظه بیشتری نیز نیاز خواهند داشت . با استفاده از دستور Show version می توان وضعیت image موجود و حافظه فلش را مشاهده نمود . قبل از نصب یک نسخه جدید از نرم افزار IOS ، می بایست وضعیت حافظه آن به منظور اطمینان از وجود ظرفیت کافی ، بررسی گردد.

برای مشاهده میزان حافظه RAM ، از دستور Show version استفاده می گردد:

دستور تایپ	خروجی
Router>Show Version	..... System image file is "flash:c2600-dos-mz_120-4_T.bin" Processor board ID JAB040202ZW (201830944) M860 processor: part number 0, mask 49 Bridging software. X.25 software, Version 3.0.0. 2 FastEthernet/IEEE 802.3 interface(s) 32K bytes of non-volatile configuration memory. 8192K bytes of processor board System flash (Read/Write) Configuration register is 0x2102

برای مشاهده میزان حافظه فلش می توان از دستور Show flash استفاده نمود.

دستور تایپ	خروجی
Router>show flash	System flash directory: File Length Name/status 1 6399468 c2600-dos-mz_120-4_T.bin [6399532 bytes used, 1989076 available, 8388608 total] 8192K bytes of processor board System flash (Read/Write)

راه اندازی روتر : ایجاد یک Hyper Terminal Session

تمامی روترهای سیسکو دارای یک پورت کنسول سریال غیرهمزمان TIA/EIA-232 می باشند. برای اتصال یک ترمینال به پورت کنسول روتر، از کابل ها و آداپتورهای خاصی استفاده می گردد: ترمینال، یک ترمینال اسکی و یا کامپیوتری است که بر روی آن نرم افزارهای شبیه ساز ترمینال نظیر HyperTerminal اجراء شده باشد. برای اتصال کامپوتر به پورت کنسول روتر از RJ-45 to RJ-45 rollover cable به همراه آداپتور RJ-45 to DB-9 استفاده می گردد.

نرم افزارهای شبیه ساز ترمینال

هر سیستم عامل از یک و یا چندین نوع برنامه شبیه ساز ترمینال استفاده می نماید. HyperTerminal ، یک برنامه ساده شبیه ساز ترمینال است که از آن در نسخه های مختلف ویندوز اسفاده می گردد. در واقع، کامپیوتر به همراه HyperTerminal ، نظیر یک ترمینال رفتار می نماید (با استفاده از صفحه کلید فرامین تایپ و پس از ارسال به روتر، نتایج از طریق نمایشگر کامپیوتر، نمایش داده می شود).

استفاده از یک کابل rollover و برنامه ای نظیر HyperTerminal ، متداولترین روش اتصال به پورت کنسول روتر به منظور بررسی و تغییر پارامترهای پیکربندی روتر می باشد.

تجهیزات مورد نیاز

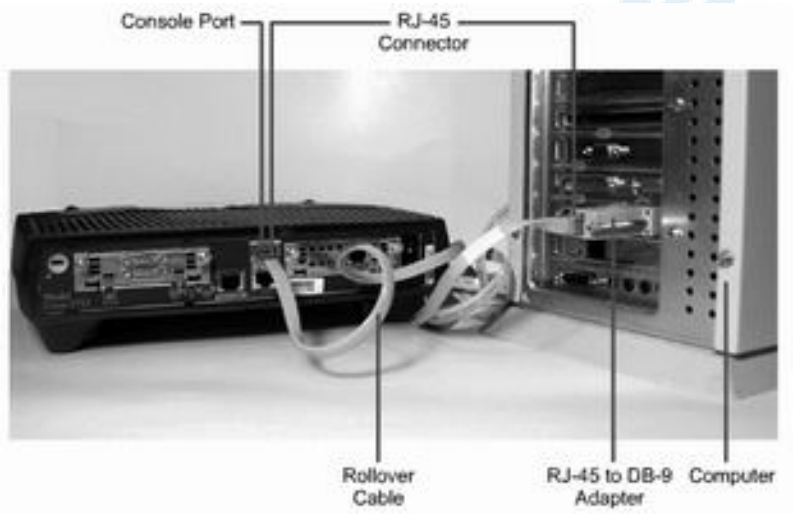
برای اتصال کامپیوتر به روتر به تجهیزات و امکانات زیر نیاز می باشد :

- یک دستگاه کامپیوتر که دارای یک اینترفیس سریال است و برنامه HyperTerminal بر روی نصب شده باشد .
- یک روتر
- کابل کنسول و یا rollover برای اتصال کامپیوتر به روتر

ایجاد یک HyperTerminal Session

برای ایجاد یک HyperTerminal Session و اتصال کامپیوتر به روتر مراحل زیر را دنبال می نمائیم :

مرحله اول – پیکربندی اولیه روتر : در اولین اقدام می بایست کابل rollover را به پورت کنسول روتر و سر دیگر آن را با استفاده از یک آداپتور DB-9 و یا DB-25 به پورت سریال (COM) کامپیوتر متصل نمود.



اتصال روتر به کامپیوتر (منبع : سایت سیسکو)

مرحله دوم – اجرای برنامه HyperTerminal : در این مرحله پس از روشن کردن کامپیوتر و روتر ، برنامه HyperTerminal موجود در مسیر زیر را اجراء می نمائیم .

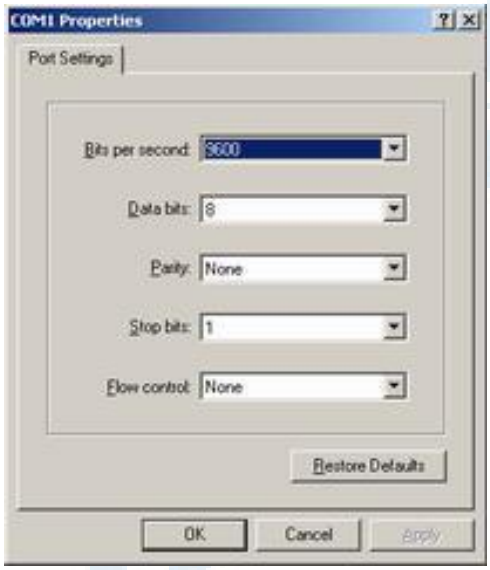
```
Start > Programs > Accessories > Communications > Hyper Terminal
```

مرحله سوم – انتخاب یک نام برای HyperTerminal Session : در این مرحله برای ارتباط مورد نظر ، یک نام را مشخص می نمائیم.

مرحله چهارم –انتخاب اینترفیس ارتباطی کامپیوتر : در این مرحله نوع اینترفیس ارتباطی کامپیوتر با روتر را مشخص می نمائیم (پورت سریال : COM1).

مرحله پنجم – مشخص نمودن خصایص اینترفیس ارتباطی : در این مرحله خصایص پورت سریال انتخاب شده در مرحله قبل (COM1) را مشخص می نمائیم .

- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None



پس از فعال شدن پنجره HyperTerminal session ، روتر را روشن نموده و در صورتی که روتر روشن است ، کلید Enter را فعال و در انتظار پاسخ روتر می مانیم . در صورت پاسخ روتر ، یک ارتباط موفقیت آمیز با روتر برقرار شده است.

مرحله ششم : بستن Session : برای خاتمه دادن به Console session ، گزینه Exit را از طریق منوی Exit انتخاب نموده و آن را با یک نام دلخواه ذخیره می نمائیم (استفاده مجدد از آن در آینده).

آشنائی با عناصر داخلی روتر

روتر یکی از دستگاه های شبکه ای مهم و حیاتی است که از آن در شبکه های LAN و WAN استفاده می گردد. روترها تاکنون در مدل های متفاوت و با معماری مختلف طراحی، تولید و عرضه شده اند. در این مطلب با عناصر اصلی داخلی یک روتر آشنا خواهیم شد.

عناصر داخلی روتر

- **پردازنده (CPU)** : پردازنده مسئولیت اجرای دستورالعمل ها در سیستم عامل را برعهده دارد . مقداردهی اولیه سیستم، عملیات روتینگ و کنترل اینترفیس شبکه از جمله وظایف یک پردازنده می باشد. CPU، یک ریزپردازنده است و در روترهای بزرگ ممکن است از چندین پردازنده استفاده گردد.
- **حافظه اصلی (RAM)** : از حافظه فوق به منظور ذخیره اطلاعات جدول روتینگ ، صف های بسته های اطلاعاتی، اجراء پیکربندی و cache سوئیچینگ سریع استفاده می‌گردد. در اکثر روترها ، حافظه RAM فضای زمان اجراء برای نرم افزار IOS و زیر سیستم های مربوطه را فراهم می نماید. حافظه RAM منطقا" به دو بخش حافظه پردازنده اصلی و حافظه ورودی و خروجی مشترک تقسیم می گردد. ازحافظه ورودی و خروجی مشترک (Shared I/O) توسط اینترفیس ها و به منظور ذخیره موقت بسته های اطلاعاتی استفاده می گردد. با توجه به تکنولوژی استفاده شده در ساخت اینگونه حافظه ها، پس از خاموش کردن و یا راه اندازی مجدد روتر اطلاعات موجود در حافظه RAM حذف می گردد. حافظه های فوق معمولا" از نوع DRAM (حافظه RAM پویا) بوده و می توان با افزودن ماژول های DIMMs ظرفیت آنان را تغییر و افزایش داد.

- **حافظه فلش (Flash)** : از این نوع حافظه ها به منظور ذخیره نسخه کامل نرم افزار IOS استفاده می گردد. روتر، معمولاً" IOS پیش فرض خود را از حافظه فلش دریافت می نماید. با توجه به تکنولوژی استفاده شده در ساخت اینگونه حافظه ها، همواره می توان نرم افزار ذخیره شده درون آنان را ارتقاء و با یک نسخه جدید جایگزین نمود. IOS ممکن است به صورت فشرده و یا معمولی ذخیره شده باشد . در اکثر روترها یک نسخه اجرائی از IOS در زمان راه اندازی روتر به حافظه RAM انتقال می یابد. در سایر روترها، IOS ممکن است مستقیماً" از طریق حافظه فلش اجراء گردد. با افزودن و یا تعویض ماژول های SIMMs و یا کارت های PCMCIA می توان ظرفیت حافظه فلش را ارتقاء داد.
- **حافظه NVRAM** : از این نوع حافظه های غیر فرار به منظور ذخیره پیکربندی راه اندازی روتر استفاده می گردد. در برخی دستگاه ها، NVRAM بر اساس تکنولوژی EEPROMs و در سایر دستگاه ها به صورت حافظه های فلش پیاده سازی می گردد. اطلاعات موجود درNVRAM پس از خاموش شدن و یا راه اندازی مجدد روتر از بین نخواهند رفت.
- **گذرگاه ها (Buses)** : اکثر روترها شامل یک گذرگاه سیستم و یک گذرگاه پردازنده می‌باشند . از گذرگاه سیستم به منظور مبادله اطلاعات بین پردازنده و اینترفیس ها و یا تجهیزات جانبی نصب شده در یکی از اسلات های سیستم، استفاده می گردد . گذرگاه فوق مسئولیت مبادله بسته های اطلاعاتی به اینترفیس ها را برعهده دارد (دریافت و ارسال).

  گذرگاه پردازنده توسط پردازنده و به منظور دستیابی عناصر از طریق حافظه اصلی روتر استفاده می گردد. این گذرگاه مسئولیت مبادله دستورالعمل ها و داده به یک آدرس خاص از حافظه را برعهده دارد (ذخیره و بازیابی).

- **حافظه ROM** : از این نوع حافظه به منظور ذخیره دائم کد اشکال زدائی راه انداز (ROM Monitor) استفاده می‌گردد . مهمترین وظیفه حافظه ROM ، تست و عیب یابی سخت افزار در زمان راه اندازی روتر و استقرار نرم افزار IOS از حافظه فلش به درون حافظه RAM می‌باشد. برخی روترها دارای یک نسخه خاص و سبک تر از IOS می باشند که می توان از آن به عنوان یک گزینه و منبع جایگزین در زمان راه اندازی روتر استفاده نمود. اطلاعات موجود در اینگونه حافظه ها را نمی توان حذف نمود و در صورت نیاز به ارتقاء ، می‌بایست تراشه مربوطه را تعویض نمود .
- **اینترفیس ها** : اینترفیس ها مسئولیت اتصالات روتر به دنیای خارج را برعهده داشته و می توان آنان را به سه گروه عمده تقسیم نمود:
  اینترفیس های مختص شبکه محلی : این نوع اینترفیس ها معمولا" یکی از گزینه های متفاوت اترنت و یا Token Ring می باشند . اینترفیس های فوق دارای تراشه های کنترلی خاصی می باشند که منطق لازم برای اتصال سیستم به محیط انتقال را ارائه می نمایند. پیکربندی اینترفیس های فوق ممکن است به صورت ثابت و یا ماژولار (پیمانه ای و قابل افزایش با توجه به نیاز) باشد.
  اینترفیس های مختص شبکه WAN : شامل اینترفیس های سریال، ISDN و CSUs (برگرفته از Channel Service Unit) می باشد. همانند اینترفیس شبـــکه های محلی، این نوع اینترفیس ها نیز دارای تراشـــــه های کنترلی خاصی می باشند که منطق لازم برای اتصال سیستم به محیط انتقال را ارائه می نمایند. پیکربندی اینترفیس های فوق ممکن است به صورت ثابت و یا ماژولار باشد.
  اینترفیس های کنسول و کمکی : این نوع اینترفیس ها، پورت های سریالی می باشند که از آنان جهت پیکربندی اولیه روتر استفاده می گردد. پورت های فوق را نمی توان به عنوان پورت های شبکه در نظر گرفت و از آنان صرفا" جهت

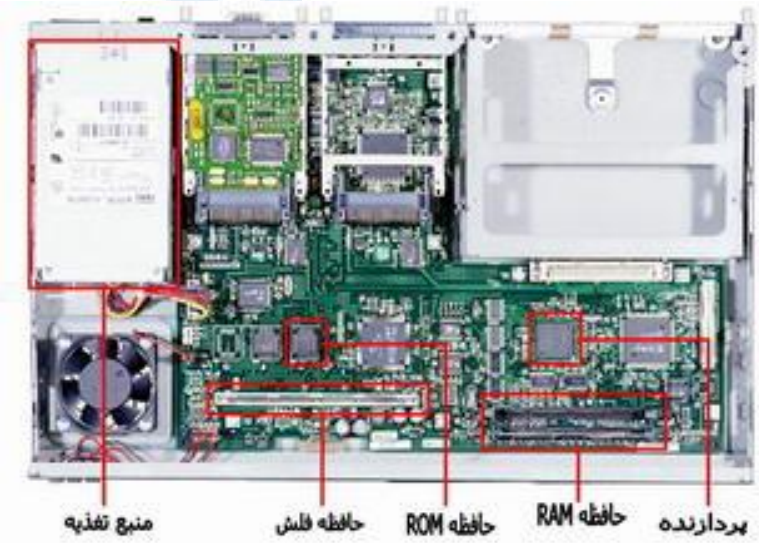
برقراری ارتباط از طریق پورت های ارتباطی کامپیوتر و یا مودم استفاده بعمل می آید.

- **منبع تغذیه** : منبع تغذیه توان لازم برای عملکرد صحیح عناصر داخلی روتر را تامین می نماید. روترهای بزرگ ممکن است دارای چندین منبع تغذیه باشند. در روترهای کوچک منبع تغذیه ممکن است به صورت External باشد.

محل نصب عناصر داخلی درون روتر

برای استفاده از روتر لازم نیست که با محل نصب عناصر اشاره شده درون روتر آشنا باشیم ولی در برخی موارد نظیر ارتقاء حافظه این موضوع می تواند ضرورت خاص خود را داشته باشد .

نوع عناصر و محل نصب آنان در روترها با توجه به مدل آنان می تواند متفاوت و متغیر باشد . شکل زیر عناصر اصلی داخلی در یک روتر ۲۶۰۰ را نشان می دهد.



عناصر اصلی داخلی روتر ۲۶۰۰ (منبع : سایت سیسکو)

شکل زیر برخی کانکتورهای خارجی یک روتر ۲۶۰۰ را نشان می دهد.

کانکتورهای خارجی روتر ۲۶۰۰ (منبع : سایت سیسکو)

آشنائی با اینترفیس های روتر

اینترفیس ها مسئولیت اتصالات روتر به دنیای خارج را برعهده داشته و می توان آنان را به سه گروه عمده اینترفیس های مختص شبکه محلی، اینترفیس های مختص شبکه WAN و اینترفیس های کنسول و کمکی تقسیم نمود. در این مطلب با اینترفیس های فوق آشنا خواهیم شد.

انواع اینترفیس های روتر

اینترفیس ها مسئولیت اتصالات روتر به دنیای خارج را برعهده داشته و می توان آنان را به سه گروه عمده تقسیم نمود:

- **اینترفیس های مختص شبکه محلی** : با استفاده از اینترفیس های فوق یک روتر می تواند به محیط انتقال شبکه محلی متصل گردد. اینگونه اینترفیس ها معمولا" نوع خاصی از اترنت می باشند. در برخی موارد ممکن است از سایر تکنولوژی های LAN نظیر Token Ring و یا ATM (برگرفته از Asynchronous Transfer Mode) نیز استفاده گردد.
- **اینترفیس های مختص شبکه WAN** : این نوع اینترفیس ها اتصالات مورد نیاز از طریق یک ارائه دهنده سرویس به یک سایت خاص و یا اینترنت را فراهم می نمایند . اتصالات فوق ممکن است از نوع سریال و یا هر تعداد دیگر از اینترفیس های WAN باشند. در زمان استفاده از برخی اینترفیس های WAN ، به یک دستگاه خارجی نظیر CSU به منظور اتصال روتر به اتصال محلی ارائه دهنده سرویس نیاز می باشد. در برخی دیگر از اتصالات WAN ، ممکن است روتر مستقیما" به ارائه دهنده سرویس متصل گردد.
- **اینترفیس های کنسول و کمکی** : عملکرد پورت های مدیریتی متفاوت از سایر اتصالات است . اتصالات LAN و WAN ، مسولیت ایجاد اتصالات شبکه ای به

منظور ارسال فریم ها را برعهده دارند ولی پورت های مدیریتی یک اتصال مبتنی بر متن به منظور پیکربندی و اشکال زدائی روتر را ارائه می نمایند. پورت های کمکی (auxilliary) و کنسول (console) دو نمونه متداول از پورت های مدیریت روتر می باشند . این نوع پورت ها، از نوع پورت های سریال غیرهمزمان EIA-232 می باشند که به یک پورت ارتباطی کامپیوتر متصل می گردند. در چنین مواردی از یک برنامه شبیه ساز ترمینال بر روی کامپیوتر به منظور ایجاد یک ارتباط مبتنی بر متن با روتر استفاده می گردد . مدیران شبکه می توانند با استفاده از ارتباط ایجاد شده مدیریت و پیکربندی دستگاه مورد نظر را انجام دهند.

شکل زیر انواع اتصالات یک روتر را نشان می دهد.

انواع اینترفیس یک روتر (منبع : سایت سیسکو)

در ادامه با نحوه استفاده از اینترفیس های فوق آشنا خواهیم شد.

پیکربندی روتر با استفاده از پورت های مدیریت

پورت های کنسول و کمکی به منزله پورت های مدیریتی می باشند که از آنان به منظور مدیریت و پیکربندی روتر استفاده می گردد. این نوع پورت های سریال غیرهمزمان به عنوان پورت های شبکه ای طراحی نشده اند. برای پیکربندی اولیه روتر از یکی از پورت های فوق استفاده می گردد. معمولا" برای پیکربندی اولیه، استفاده از پورت کنسول توصیه می گردد چراکه تمامی روترها ممکن است دارای یک پورت کمکی نباشند. زمانی که روتر برای اولین مرتبه وارد مدار و یا سرویس می گردد، با توجه به عدم وجود پارامترهای پیکربندی شده ، امکان برقراری ارتباط با هیچ شبکه ای وجود نخواهد داشت.

برای پیکربندی و راه اندازی اولیه روتر ، می توان از یک ترمینال و یا کامپیوتر که به پورت کنسول روتر متصل می گردد، استفاده نمود. پس از اتصال کامپیوتر به روتر ، می توان با استفاده از دستورات پیکربندی، تنظیمات مربوطه را انجام داد. پس از پیکربندی روتر با استفاده از پورت کنسول و یا کمکی، زمینه اتصال روتر به شبکه به منظور اشکال زدائی و یا مانیتورینگ فراهم می گردد.

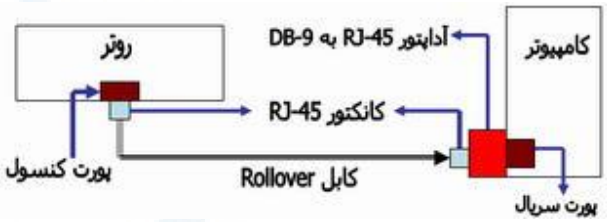
نحوه اتصال به پورت کنسول روتر

برای اتصال کامپیوتر به پورت کنسول روتر ، به یک کابل rollover و یک آداپتور RJ-45 to DB-9 نیاز می باشد. روترهای سیسکو به همراه آداپتورهای مورد نیاز برای اتصال به پورت کنسول ارائه می گردند. کامپیوتر و یا ترمینال می بایست قادر به حمایت از شبیه سازی ترمینال VT100 باشند. در این رابطه از نرم افزارهای شبیه ساز ترمینال نظیر HyperTerminal استفاده می‌گردد.

برای اتصال کامپیوتر به روتر می بایست مراحل زیر را دنبال نمود:

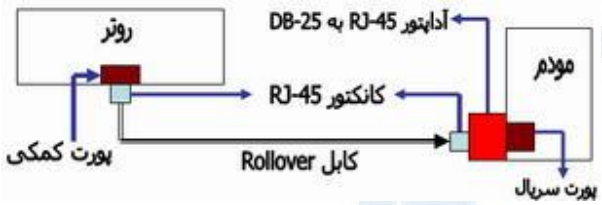
- پیکربندی نرم افزار شبیه سازی ترمینال بر روی کامپیوتر (انتخاب شماره پورت مناسب و ...)
- اتصال کانکتور RJ-45 کابل rollover به پورت کنسول روتر
- اتصال سر دیگر کابل rollover به آداپتور RJ-45 to DB-9
- اتصال آداپتور DB-9 به کامپیوتر

شکل زیر نحوه اتصال کامپیوتر به روتر را با استفاده از یک کابل rollover نشان می دهد :



اتصال کامپیوتر به روتر

برای مدیریت و پیکربندی از راه دور روتر، می توان یک مودم را به پورت کنسول و یا کمکی روتر متصل نمود. شکل زیر نحوه اتصال روتر به یک مودم را نشان می دهد :



ارتباط با روتر از طریق مودم

به منظور اشکال زدائی روتر، استفاده از پورت کنسول نسبت به پورت کمکی ترجیح داده می شود. در زمان استفاده از پورت کنسول به صورت پیش فرض پیام های خطاء، اشکال زدائی و راه اندازی نمایش داده می شوند. از پورت کنسول در مواردی که سرویس های شبکه فعال نشده و یا با مشکل مواجه شده اند نیز می توان استفاده نمود. بنابراین پورت کنسول گزینه ای مناسب برای بازیافت رمز عبور و سایر مشکلات غیرقابل پیش بینی می باشد.

اتصال اینترفیس های LAN

در اکثر محیط های LAN ، روتر با استفاده از یک اینترفیس Ethernet و یا Fast Ethernet به شبکه متصل می گردد. در چنین مواردی روتر همانند یک میزبان است که با شبکه LAN از طریق یک هاب و یا سوئیچ ارتباط برقرار می نماید. به منظور ایجاد اتصال از یک کابل straight-through استفاده می گردد. دربرخی موارد، اتصال

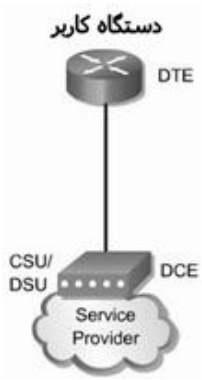
اترنت روتر مستقیما"به کامپیوتر و یا روتر دیگری متصل می گردد. در چنین مواردی از یک کابل Crossover استفاده می گردد.

در صورت عدم استفاده صحیح از اینترفیس ها، ممکن است روتر و یا سایر تجهیزات شبکه ای با مشکل مواجه گردند.

اتصال اینترفیس های WAN

اتصالات WAN دارای انواع مختلفی بوده و از تکنولوژی های متفاوتی استفاده می نمایند. سرویس های WAN معمولا" از ارائه دهندگان سرویس اجاره می گردد. خطوط leased و یا packet-switched نمونه هائی از انواع متفاوت اتصالات WAN می باشند.

برای هر یک از انواع سرویس های WAN ، دستگاه مشتری (اغلب یک روتر است) به منزله یک DTE (برگرفته از data terminal equipment) رفتار می نماید. پایانه فوق با استفاده از یک دستگاه DCE (برگرفته از data circuit-terminating equipment) که معمولا" یک مودم و یا CSU/DSU (برگرفته از channel service unit/data service unit) می باشد به ارائه دهنده سرویس متصل می گردد. از دستگاه فوق برای تبدیل داده از DTE به یک شکل قابل قبول برای ارائه دهنده سرویس WAN ، استفاده می گردد.



استفاده از اینترفیس WAN (منبع : سایت سیسکو)

اینترفیس های سریال، متداولترین اینترفیس استفاده شده در روتر برای سرویس های WAN می باشند. برای انتخاب کابل سریال مناسب، بررسی موارد زیر پیشنهاد می گردد:

- **نوع اینترفیس** : روترهای سیسکو ممکن است از کانکتورهای متفاوتی برای اینترفیس های سریال استفاده نمایند. مثلا" در برخی روترها از اینترفیس های سریال smart و یا یک اتصال DB-60 استفاده می گردد.
- **نوع اتصال شبکه** : آیا شبکه به یک دستگاه DCE و یا DTE متصل است؟ DCE و DTE دو نوع اینترفیس سریال می باشند که دستگاه ها از آنان به منظور ارتباط با یکدیگر استفاده می نمایند . ارائه سیگنال کلاک برای مبادله اطلاعات بر روی گذرگاه، مهمترین ویژگی دستگاه های DTE محسوب می گردد.
- **نوع سیگنالینگ** : برای هر دستگاه می توان از یک استاندارد سریال متفاوت استفاده نمود. هر استاندارد، سیگنال های موجود بر روی کابل را تعریف و نوع کانکتورهای دو سر کابل را مشخص می نماید.

روتر و جایگاه آن در شبکه های WAN

روتر یکی از دستگاه های شبکه ای مهم و حیاتی است که از آن در شبکه های LAN و WAN استفاده می گردد. در این مطلب پس از آشنائی اولیه با روتر، با جایگاه آن در شبکه های WAN آشنا خواهیم شد.

آشنائی اولیه با روتر

روتر یک نوع کامپیوتر خاص است که دارای عناصر مشابه یک کامپیوتر استاندارد شخصی نظیر پردازنده، حافظه، خطوط داده و اینترفیس های مختلف ورودی و خروجی است. روترها به منظور انجام عملیات بسیار خاص که عموما" نمی توان آنان را توسط کامپیوترهای شخصی انجام داد، طراحی شده اند. مثلا" با استفاده از روتر می توان دو شبکه را به یکدیگر متصل تا در ادامه امکان مبادله اطلاعات بین آنان فراهم گردد. روتر، همچنین بهترین مسیر ارسال داده از یک شبکه به شبکه ای دیگر را تعیین می نماید. کامپیوترها به منظور اجرای برنامه های نرم افزاری به یک سیستم عامل نیاز دارند، این وضعیت در روترها نیز وجود داشته و آنان نیز جهت اجرای فایل های پیکربندی به یک سیستم عامل که به آن IOS (برگرفته از Internetwork Operating System software) گفته می شود، نیاز خواهند داشت. فایل های پیکربندی شامل دستورالعمل ها و پارامترهائی می باشند که بر اساس آنان ترافیک ورودی و خروجی روتر کنترل می گردد. مثلا" روترها با استفاده از پروتکل های روتینگ، قادر به اتخاذ تصمیم مناسب در خصوص بهترین مسیر بسته های اطلاعاتی می باشند.

حافظه های RAM ، NVRAM ، فلش، ROM و اینترفیس ها مهمترین عناصر داخلی یک روتر می باشند که در ادامه به بررسی هر یک از آنان خواهیم پرداخت.

حافظه RAM (برگرفته از **random access memory**) : حافظه RAM که به آن DRAM (حافظه RAM پویا) نیز گفته می‌شود دارای خصوصیات و وظایف زیر می باشد :

- ذخیره جداول روتینگ
- نگهداری Cache ARP
- نگهداری fast-Switching cache
- نگهداری و پشتیبانی از صف های حاوی بسته های اطلاعاتی
- ارائه حافظه موقت برای فایل پیکربندی در زمان روشن کردن روتر
- عدم نگهداری اطلاعات پس از خاموش کردن و یا راه اندازی مجدد روتر

حافظه NVRAM (برگرفته از **nonvolatile random-access memory**) : حافظه NVRAM یا غیرفرار دارای خصایص و وظایف زیر می باشد :

- محل نگهداری فایل پیکربندی راه اندازی روتر
- نگهداری اطلاعات پس از خاموش کردن و یا راه اندازی مجدد روتر

حافظه فلش : حافظه فلش دارای خصایص و وظایف زیر می باشد:

- نگهداری IOS (سیستم عامل)
- بهنگام سازی نرم افزار بدون ضرورت تعویض و یا جایگزینی تراشه های موجود بر روی پردازنده
- نگهداری اطلاعات پس از خاموش کردن و یا راه اندازی مجدد روتر
- قابلیت ذخیره چندین نسخه از نرم افزار IOS

- امکان حذف اطلاعات (یک نوع خاص از حافظه های ROM با قابلیت حذف الکترونیکی اطلاعات: EEPROM)

حافظه ROM (برگرفته از Read-only memory)، حافظه ROM و یا فقط خواندنی دارای خصایص و وظایف زیر می باشد:

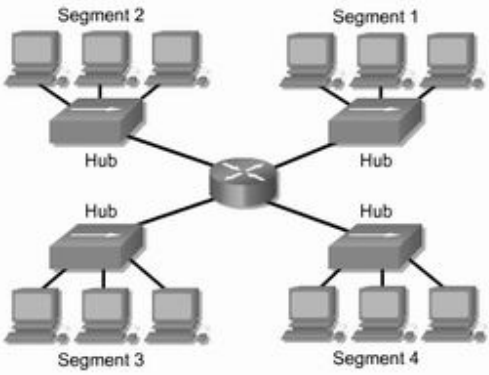
- نگهداری دستورالعمل های لازم برای اشکال زدائی و اجرای برنامه POST (برگرفته از power-on self test)
- ذخیره برنامه راه اندازی روتر موسوم به bootstrap و نرم افزار اولیه سیستم عامل
- تعویض تراشه های موجود بر روی برد اصلی در صورت نیاز به ارتقاء نرم افزار ذخیره شده

اینترفیس ها : اینترفیس ها دارای خصایص و وظایف زیر می باشند:

- روتر را به شبکه متصل می نمایند (ورود و خروج فریم ها).
- اینترفیس ها ممکن است بر روی برد اصلی و یا به عنوان ماژول های جداگانه ارائه گردند .

جایگاه روتر در شبکه های LAN و WAN

با این که می توان از روتر برای تقسیم (Segmentation) یک شبکه محلی استفاده نمود ولی مهمترین کاربرد آن به عنوان یک دستگاه شبکه ای در شبکه های WAN می باشد. شکل زیر نحوه استفاده از روتر دریک شبکه محلی را نشان می دهد.



استفاده از روتر دریک شبکه محلی (منبع : سایت سیسکو)

از تکنولوژی های WAN در اکثر موارد به منظور اتصال روترها به یکدیگر استفاده می گردد و روترها با اتصالات مبتی بر WAN با یکدیگر ارتباط برقرار می نمایند. روترها مسئولیت ایجاد ستون فقرات در شبکه های داخلی بزرگ (اینترانت) و یا اینترنت را برعهده داشته و در لایه سوم مدل مرجع OSI فعالیت می نمایند (اتخاذ تصمیم بر اساس آدرس های شبکه).

انتخاب بهترین مسیر و سوئیچینگ فریم ها به اینترفیس مناسب از مهمترین وظایف یک روتر محسوب می گردد. روترها به منظور انجام وظایف فوق جداول روتینگی را ایجاد (ایستا و یا پویا) تا به کمک آن اقدام به مبادله اطلاعات شبکه با سایر روترها نمایند . یک مدیر شبکه می تواند با پیکربندی مسیرهای ایستا، اطلاعات جداول روتینگ را سازماندهی و مدیریت نماید ولی عموما" اطلاعات موجود در جداول روتینگ به صورت پویا و با استفاده از یک پروتکل روتینگ ذخیره و بهنگام می گردند. مسئولیت پروتکل روتینگ ، مبادله اطلاعات توپولوژی شبکه (مسیر) با سایر روترها می باشد. یک شبکه به منظور ارتباط با سایر شبکه ها می بایست به درستی پیکربندی گردد. این چنین شبکه هائی امکانات زیر را ارائه می نمایند:

- آدرس دهی پیوسته و سازگار
- انتخاب بهترین مسیر

- روتینگ ایستا و یا پویا
- سوئیچینگ
- آدرس هائی که بیانگر توپولوژی های شبکه می باشند.

جایگاه روتر در شبکه های WAN

شبکه های WAN در لایه فیزیکی و data link مدل مرجع OSI فعالیت می نمایند. مطلب فوق بدین معنی نمی باشد که پنج لایه دیگر مدل مرجع OSI در شبکه های WAN جایگاهی ندارند . عبارت فوق بر این نکته مهم تاکید می نماید که خصایصی که یک شبکه WAN را از LAN متمایز می نماید در لایه های فیزیکی و link data حضور موثر و کاملا" مشهودی را دارند. به عبارت دیگر، استانداردها و پروتکل های استفاده شده در شبکه های WAN و در لایه های اول و دوم متفاوت با استانداردها و پروتکل های استفاده شده در شبکه های محلی و در لایه های مشابه می باشد. لایه فیزیکی WAN، اینترفیس بین DTE (برگرفته از data terminal equipment) و DCE (برگرفته از data circuit equipment) را تشریح می نماید. عموما" ، DCE یک ارائه دهنده سرویس و DTE دستگاه ضمیمه می باشد. به عبارت دیگر DTE ، دستگاه کاربر با اینترفیس مربوطه است که به لینک WAN متصل می گردد. در این مدل، سرویس های ارائه شده به DTE از طریق یک مودم و یا CSU/DSU در دسترس قرار می گیرد.

وظیفه اصلی یک روتر، روتینگ است و روتینگ در لایه شبکه و یا لایه سوم مدل مرجع OSI محقق می گردد ولی اگر یک شبکه WAN در لایه های اول و دوم مدل مرجع OSI فعالیت می نماید ، آیا روتر یک دستگاه شبکه محلی و یا یک دستگاه WAN است ؟ در پاسخ به سوال فوق می بایست گفت که هر دو گزینه درست می باشند. یک روتر ممکن است انحصارا" به عنوان یک دستگاه شبکه محلی ایفای وظیفه نماید و یا ممکن است منحصرا" وظیفه یک دستگاه WAN را در شبکه برعهده داشته باشد و یا در برخی

موارد که در محدوده مرزی بین یک شبکه LAN و WAN استفاده می گردد، در یک لحظه می‌تواند هم به عنوان یک دستگاه شبکه محلی و هم به عنوان یک دستگاه WAN وظایف محوله را انجام دهد .

یکی از وظایف روتر در شبکه های WAN ، مسیردهی بسته های اطلاعاتی در لایه سوم است ولی روتر در یک شبکه محلی نیز دارای چنین مسئولیتی است . بنابراین نمی توان روتینگ را به عنوان یک وظیفه اختصاصی برای روتر در شبکه های WAN در نظر گرفت. زمانی که یک روتر از استانداردها و پروتکل های مرتبط با WAN در لایه های فیزیکی و data link استفاده می نماید، وی به عنوان یک دستگاه WAN در شبکه ایفای وظیفه می نماید. اولین وظیفه روتر در یک شبکه WAN روتینگ نمی باشد و اگر قرار است برای آن وظیفه ای اختصاصی را تعریف نمائیم بهتر است گفته شود که مسئولیت روتر در شبکه های WAN ، ارائه اتصالات لازم بین استانداردهای مختلف data link و فیریکی WAN است.

مثلا" یک روتر ممکن است دارای یک اینترفیس ISDN باشد که از کپسوله سازی PPP استفاده می نماید و همچنین دارای یک اینترفیس سریال T1 باشد که در آن از کپسوله سازی Frame Relay استفاده می گردد . در چنین وضعیتی روتر می بایست قادر به انتقال بیت ها از یک نوع سرویس (نظیر ISDN) به سرویس دیگر (نظیر T1) و تغییر کپسوله سازی data link از PPP به Frame Relay باشد.

استانداردها و پروتکل های لایه فیزیکی و data link در شبکه های WAN

برخی‌از پروتکل ها و استانداردهای لایه فیزیکی عبارتند از:

- EIA/TIA-232
- EIA/TIA-449
- V.24
- V.35
- X.21
- G.703

- EIA-530
- ISDN
- T1, T3, E1, and E3
- xDSL
- SONET (OC-3, OC-12, OC-48, OC-192)

برخی از پروتکل ها و استانداردهای لایه data link عبارتند از :

- High-level data link control (HDLC)
- Frame Relay
- Point-to-Point Protocol (PPP)
- Synchronous Data Link Control (SDLC)
- Serial Line Internet Protocol (SLIP)
- X.25
- ATM
- LAPB
- LAPD
- LAPF

انواع روتر

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

انواع روترها

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

- **روترهای سخت افزاری** : روترهای فوق، سخت افزارهائی می باشند که نرم افزارهای خاص تولید شده توسط تولید کنندگان را اجراء می نمایند (درحال حاضر صرفا" به صورت black box به آنان نگاه می کنیم).نرم افزار فوق، قابلیت روتینگ را برای روترها فراهم نموده تا آنان مهمترین و شاید ساده ترین وظیفه خود که ارسال داده از یک شبکه به شبکه دیگر است را بخوبی انجام دهند. اکثر شرکت ها ترجیح می دهند که از روترهای سخت افزاری استفاده نمایند چراکه آنان در مقایسه با روترهای نرم افزاری، دارای سرعت و اعتماد پذیری بیشتری می باشند. شکل زیر یک نمونه روتر را نشان می دهد. (Cisco 2600 Series Multiservice Platform)

منبع : سایت سیسکو

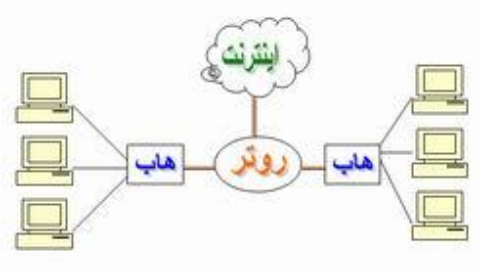
- **روترهای نرم افزاری** : روترهای نرم افزاری دارای عملکردی مشابه با روترهای سخت افزاری بوده و مسئولیت اصلی آنان نیز ارسال داده از یک شبکه به شبکه دیگر است. یک روتر نرم افزاری می تواند یک سرویس دهنده NT ، یک سرویس دهنده نت ور و یا یک سرویس دهنده لینوکس باشد. تمامی سیستم های عامل شبکه ای مطرح ،دارای قابلیت های روتینگ از قبل تعبیه شده می باشند.

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

مثال ۱ : استفاده از روتر به منظور اتصال دو شبکه به یکدیگر و ارتباط به اینترنت

فرض کنید از یک روتر مطابق شکل زیر به منظور اتصال دو شبکه LAN به یکدیگر و اینترنت، استفاده شده است. زمانی که روتر داده ای را از طریق یک شبکه LAN و یا اینترنت دریافت می نماید، پس از بررسی آدرس مبداء و مقصد، داده دریافتی را برای هر یک از شبکه ها و یا اینترنت ارسال می نماید. روتر استفاده شده در شکل زیر ، شبکه را

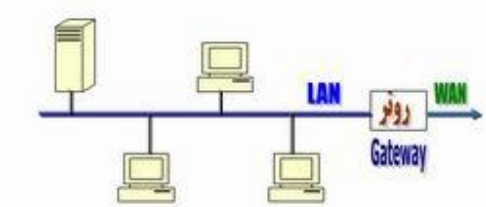
به دو بخش متفاوت تقسیم نموده است. (دو شبکه مجزاء). هر شبکه دارای یک هاب است که تمامی کامپیوترهای موجود در شبکه به آن متصل شده اند. علاوه بر موارد فوق، روتر استفاده شده دارای اینترفیس های لازم به منظور اتصال هر شبکه به آن بوده و از یک اینترفیس دیگر به منظور اتصال به اینترنت، استفاده می نماید. بدین ترتیب، روتر قادر است داده مورد نظر را به مقصد درست، ارسال نماید.



مثال ۲: استفاده از روتر در یک شبکه LAN

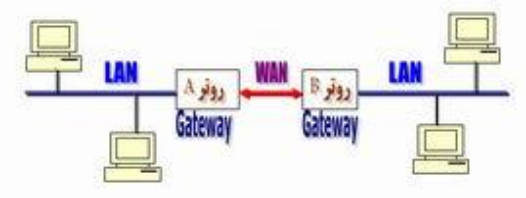
فرض کنید از یک روتر مطابق شکل زیر در یک شبکه LAN، استفاده شده است. در مدل فوق، هر یک ازدستگاههای موجود در شبکه با روتر موجود نظیر یک gateway برخورد می نمایند. بدین ترتیب، هر یک از ماشین های موجود بر روی شبکه LAN که قصد ارسال یک بسته اطلاعاتی (اینترنت و یا هر محل خارج از شبکه LAN) را داشته باشند، بسته اطلاعاتی مورد نظر را برای gateway ارسال می نمایند.

روتر (gateway) نسبت به محل ارسال داده دارای آگاهی لازم می باشد. (در زمان تنظیم خصلت های پروتکل TCP/IP برای هر یک از ماشین های موجود در شبکه یک آدرس IP برای gateway در نظر گرفته می شود). شکل زیر نحوه استفاده از یک روتر به منظور دستیابی کاربران به اینترنت در شبکه LAN را نشان می دهد:



مثال ۳: استفاده از روتر به منظور اتصال دو دفتر کار

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



مهمترین ویژگی های یک روتر :

- روترها دستگاههای لایه سوم (مدل مرجع OSI) می باشند.
- روترها مادامیکه برنامه ریزی نگردند ، امکان توزیع داده را نخواهند داشت.
- اکثر روترهای مهم دارای سیستم عامل اختصاصی خاص خود می باشند.
- روترها از پروتکل های خاصی به منظور مبادله اطلاعات ضروری خود (منظور داده نیست)، استفاده می نمایند .
- نحوه عملکرد یک روتر در اینترنت : مسیر ایجاد شده برای انجام مبادله اطلاعاتی بین سرویس گیرنده و سرویس دهنده در تمامی مدت زمان انجام تراکش ثابت و یکسان نبوده و متناسب با وضعیت ترافیک موجود و در دسترس بودن مسیر، تغییر می نماید.

روترهای سیسکو

سیسکو یکی از معتبرترین تولید کنندگان روتر و سوئیچ در سطح جهان است که از محصولات آن در مراکز شبکه ای متعددی استفاده می گردد . این شرکت تاکنون مدل های متعددی از روترها را با قابلیت های مختلفی تولید نموده است . سری ۱۶۰۰ ، ۲۵۰۰ و ۲۶۰۰ ، متداولترین نمونه در این زمینه می باشند . روترهای تولید شده توسط این شرکت از سری ۶۰۰ شروع و تا سری ۱۲۰۰۰ ادامه می یابد(در حال حاضر). شکل زیر برخی از نمونه های موجود را نشان می دهد:

سری ۱۲۰۰۰	سری ۲۶۰۰
	

منبع : سایت سیسکو

تمامی تجهیزات فوق، نرم افزار خاصی را با نام Internetwork Operating System و یا IOS اجراء می نمایند. IOS، هسته روترها واکثرسوئیچ های تولید شده توسط سیسکو، محسوب می گردد. این شرکت با رعایت اصل مهم سازگاری که از آن به عنوان یک استراتژی مهم در تولید و با نام Fusion Cisco، نام برده می شود، قصد دارد محصولات خود را بگونه ای تولید نماید که تمامی دستگاههای سیسکویک سیستم عامل یکسان را اجراء نمایند.

عناصر اصلی در یک روتر سیسکو

- اینترفیس (Interfaces) .با استفاده از اینترفیس ها، امکان استفاده از روتر فراهم می گردد.

- اینترفیس ها شامل پورت های سریال و اترنت مختلفی می باشند که از آنان به منظور اتصال روتر به شبکه LAN استفاده می گردد. هر روتر با توجه به پتانسیل های ارائه شده، دارای اینترفیس های متعددی است. برای هر یک از اینترفیس های روتر از یک نام خاص استفاده می شود. جدول زیر برخی از اسامی متداول را نشان می دهد.

اینترفیس	کاربرد
E0	**first Ethernet interface**
E1	**second Ethernet interface**
S0	**first Serial interface**
S1	**second Serial interface**
BRI 0	**first B channel for Basic ISDN**
BRI 1	**second B channel for Basic ISDN**

- در شکل زیر نمای پشت یک روتر سیسکورا به همراه اینترفیس های متفاوت آن مشاهده می نمائید . (یک روتر با قابلیت استفاده از ISDN).

منبع : سایت سیسکو

- همانگونه که مشاهده می نمائید، روتر فوق حتی دارای سوکت های مختص تلفن نیز می باشد، چراکه با توجه به این که روتر فوق از نوع ISDN می باشد، می بایست یک تلفن دیجیتالی را به یک خط ISDN متصل نمود. روتر فوق علاوه بر اینترفیس های ISDN دارای یک اینترفیس اترنت به منظور اتصال به یک دستگاه در شبکه LAN است (معمولا" یک هاب و یا یک کامپیوتر). در صورتی که اینترفیس فوق را به پورت uplink یک هاب متصل نمائید، می بایست سوئیچ کوچک موجود در پشت روتر را در حالت هاب، تنظیم نمود. در صورتی که

اینترفیس فوق را به یک دستگاه کامپیوتر متصل نمائید، می بایست وضعیت سوئیچ را در حالت node قرار داد . پورت Config و یا Console از نوع کانکتور DB9 (مادگی) بوده که با استفاده از یک کابل خاص به پورت سریال کامپیوتر متصل تا امکان پیکربندی مستقیم روتر، فراهم می گردد.

- **پردازنده (CPU)** : تمامی روترهای سیسکو دارای یک پردازنده اصلی می باشند که مسئولیت انجام عملیات اصلی در روتر را برعهده دارند . پردازنده با تولید وقفه (IRQ) با سایر عناصر موجود در روتر ارتباط برقرار می نماید. روترهای سیسکو از پردازنده های RISC موتورولا استفاده می نمایند. معمولا" درصد استفاده از پردازنده بر روی یک روتر معمولی از بیست تجاوز نمی نماید.
- **IOS** ، سیستم عامل اصلی اجراء شده بر روی روترها است. IOS بر اساس فرآیند موسوم به Bootup، لود ودر حافظه مستقرمی گردد. حجم IOS معمولا" بین دو تا پنج مگابایت بوده و این حجم می تواند با توجه به نوع روتر از میزان اشاره شده نیز تجاوز نماید. آخرین نسخه IOS در حال حاضر، نسخه شماره دوازده است . شرکت سیسکو به صورت مستمر و با هدف برطرف نمودن باگ ها و یا افزودن قابلیت های اضافه ، اقدام به ارائه نسخه های جانبی متعددی در طی هر ماه می نماید. (۱ . ۱۲ ، ۲. ۱۲).
- IOS ، قابلیت ها و پتانسیل های متعددی را در رابطه با روتر ارائه داده و می توان آن را بهنگام و یا به منظور Backup گرفتن آن را از روتر download نمود. در سری ۱۶۰۰۰ به بالا ، IOS بر روی یک حافظه فلش کارت PCMCIA ارائه شده است. حافظه فوق، در ادامه به یک اسلات موجود در پشت روتر متصل شده و از طریق آن image IOS، لود می گردد. IOS image ، معمولا" فشرده بوده و روتر می بایست آن را از حالت فشرده خارج نماید. IOS یکی از مهمترین عناصر موجود در یک روتر بوده و بدون وجود آن ، امکان استفاده از روتر وجود نخواهد داشت . به منظور استقرار IOS در حافظه ضرورتی

به داشتن یک کارت فلش (همانگونه که در خصوص روترهای سری ۱۶۰۰ اشاره گردید) نخواهد بود. بدین منظور می توان پیکربندی اکثر روترهای سیسکو را به منظور لود IOS image از طریق یک سرویس دهنده tftp شبکه و یا روتر دیگری که دارای چندین IOS image برای روترهای متفاوتی است، انجام داد. در چنین روترهائی از یک فلش کارت حافظه با ظرفیت بالا به منظور ذخیره سازی چندین ISO image ، استفاده می گردد.

- **Image RXBoot** ، که به آن Bootloader نیز گفته می شود ، چیزی بیشتر از یک نسخه کم حجم IOS نبوده که در حافظه ROM روتر مستقر می گردد . در صورتی که یک روتر دارای فلش کارت لازم به منظور لود IOS نباشد، می توان پیکربندی روتر را بگونه ای انجام داد که RXBoot image را لود نماید. با لود برنامه فوق، امکان انجام عملیات اولیه نگهداری و فعال نمودن و یا غیر فعال کردن اینترفیس های متفاوت آن فراهم می گردد.
- **حافظه RAM** ، محلی است که روتر، IOS و فایل های پیکربندی را در آن لود می نماید. عملکرد حافظه فوق مشابه حافظه RAM استفاده شده در کامپیوتر است (استقرار سیستم عامل و برنامه های کاربردی متفاوت) . میزان حافظه RAM مورد نیاز یک روتر، بستگی به اندازه IOS image و فایل های پیکربندی دارد. در اکثر موارد و در روترهای کوچک تر (سری ۱۶۰۰)، حافظه RAM استفاده شده بین دوازده تا شانزده مگابایت می باشد.این وضعیت در روترهای بزرگتر که دارای ISO image بیشتری می باشند، بین سی و دو تا شصت و چهار مگابایت خواهد بود. با توجه به استقرار جداول روتینگ در حافظه RAM ، در صورتی که جداول فوق بزرگ و پیچیده می باشند، می بایست از یک روتر با میزان حافظه RAM مناسبی استفاده گردد.
- **حافظه (NVRAM) Non-Volatile RAM** . روترها از حافظه فوق به منظور ذخیره و نگهداری اطلاعات مربوط به پیکربندی خود استفاده می نمایند.

پس از پیکربندی یک روتر، نتایج و ماحصل عملیات در NVRAM ذخیره می گردد. حجم حافظه فوق در مقایسه با حافظه های RAM، اندک می باشد. مثلا" در روترهای سری ۱۶۰۰ ، حجم حافظه فوق به هشت کیلوبایت می رسد. در روترهای بزرگتری نظیر سری ۲۶۰۰، حجم حافظه NVRAM به سی و دو کیلوبایت می رسد . پس از راه اندازی یک روتر و لود ISO image ، فایل پیکربندی از حافظه NVRAM به منظور انجام پیکربندی روتر، لود می گردد. اطلاعات موجود در این نوع از حافظه ها ، پاک نخواهد شد (حتی زمانی که روتر Reload و یا خاموش است).

- **حافظه ROM** ، از حافظه فوق به منظور راه اندازی و نگهداری روتر استفاده می گردد . حافظه فوق شامل برخی کدها نظیر Bootstrap و POST بوده که تسهیلات لازم در خصوص انجام تست های اولیه و راه اندازی را برای روتر فراهم می نماید . محتویات این حافظه را نمی توان تغییر داد (فقط خواندنی). تمامی اطلاعات موجود در حافظه ROM توسط تولید کننده ذخیره شده است.
- **حافظه فلش** ، همان کارتی است که در بخش IOS به آن اشاره گردید. این حافظه از نوع EEPROM (Electrical Eraseable Programmable Read Only Memory) ، می باشد. کارت فوق از طریق اسلاتی که در پشت یک روتر قرار دارد به روتر متصل می گردد و چیزی بیش از image IOS را در خود ذخیره نمی نماید. با استفاده از کنسول روتر می توان اطلاعاتی را در این نوع حافظه نوشت و یا اقدام به حذف برخی اطلاعات موجود نمود . حجم حافظه فوق از ٤ مگابایت در روترهای سری ۱۶۰۰ شروع شده و متناسب با مدل روتر، افزایش می یابد.
- **ریجستر پیکربندی (Configuration Register)**، نقطه شروع فرآیند راه اندازی IOS را مشخص می نماید (فلش کارت، سرویس دهنده tftp و یا صرفا" لود RXBoot image) . ریجستر فوق، شانزده بیتی است.

پیکربندی روترهای سیسکو

برای پیکربندی روترهای سیسکو، می بایست در ابتدا به بخش رابط کاربرآنان دستیابی داشت. بدین منظور، می توان از یک ترمینال و یا دستیابی ازراه دور استفاده نمود. پس از دستیابی به روتر، در اولین اقدام می بایست عملیات logging را انجام تا زمینه استفاده ازسایر دستورات به منظور مشاهده آخرین وضعیت پیکربندی و یا تغییر پیکربندی روتر فراهم گردد.

به منظور ارائه یک لایه امنیتی مناسب، امکان بالفعل کردن پتانسیل های ارائه شده (دستورات) روتر در دو mode متفاوت فراهم شده است:

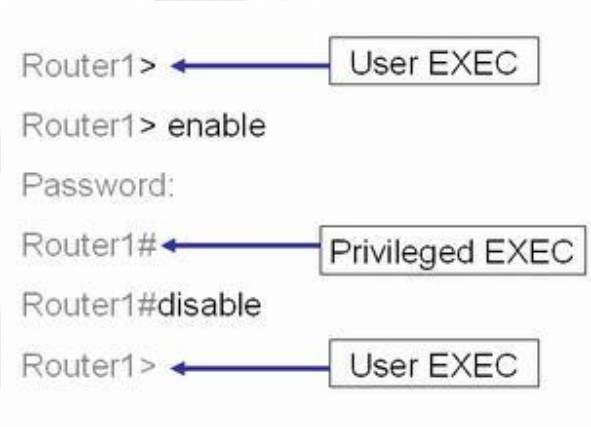
- **EXEC mode User** : در این mode ، عموما" دستوراتی را می توان اجراء نمود که ماحصل اجرای آنان، نمایش وضعیت پیکربندی روتر است و نمی توان با استفاده از مجموعه امکانات ارائه شده در این mode ، پیکربندی روتر را تغییر داد .
- **Privileged EXEC mode** : با استفاده از امکانات موجود در این mode ، می توان پیکربندی روتر را انجام و تغییرات لازم را اعمال نمود.

پس از login به روتر ، پرامپت user Exec mode نشان داده می شود . دستورات موجود در این mode ، زیرمجموعه ای از دستورات Privileged EXEC mode می باشند . برای دستیابی به مجموعه کامل دستورات می بایست به Privileged EXEC mode وارد شد. با تایپ دستور enable و یا شکل مخفف شده آن یعنی enu ، آماده ورود به این mode خواهیم شد. در صورتی که برای روتر رمز عبوری تعریف شده باشد، پس از نمایش password می بایست رمز عبور را وارد نمود. پس از تکمیل فرآیند loggin ، شکل پرامپت (prompt) تغییر و به صورت "#" نشان داده می شود که نشاندهنده ورود به Privileged EXEC mode می باشد. global

configuration mode ، یکی از حالاتی است که صرفا" از طریق Privileged EXEC mode قابل دستیابی است . امکان دستیابی به حالات زیر از طریق global configuration mode وجود دارد :

- Interface
- Subinterface
- Line
- Router
- Route-map

برای برگشت به EXEC mode از طریق Privileged EXEC mode ، از دستور disable و یا Exit استفاده می گردد . برای برگشت به Privileged EXEC mode از طریق global configuration mode ، از دستور Exit و یا کلیدهای Ctrl-Z استفاده می گردد . از ترکیب کلیدهای Ctrl-Z می توان برای برگشت مستقیم به Privileged EXEC mode از هریک از حالات زیرمجموعه global configuration mode استفاده نمود.



برای تعریف رمز عبور جهت ورود به Privileged EXEC mode، می توان از دستورات enable password و enable secret استفاده نمود. در صورت استفاده از دستورات فوق ، اولویت با دستور enable secret می باشد.

آشنائی با امکانات بخش رابط کاربر

با تایپ علامت "?" در user EXEC mode و یا privileged EXEC mode ، لیست دستورات قابل استفاده در هر mode نمایش داده می شود . دستورات صفحه به صفحه نمایش داده شده و با فشردن کلید enter می توان صفحات بعدی را مشاهده نمود.

دستورات mode user EXEC	
Exec commands: access-enable Create a temporary Access-List entry access-profile Apply user-profile to interface clear Reset functions connect Open a terminal connection disable Turn off privileged commands disconnect Disconnect an existing network connection enable Turn on privileged commands exit Exit from the EXEC help Description of the interactive help system lock Lock the terminal login Log in as a particular user logout Exit from the EXEC mrinfo Request neighbor and version information from a multicast router	**Router>?**

```
mstat Show statistics after
multiple multicast traceroutes
mtrace Trace reverse multicast
path from destination to
source
name-connection Name an
existing network connection
pad Open a X.29 PAD
connection
ping Send echo messages
ppp Start IETF Point-to-Point
Protocol (PPP)
resume Resume an active
network connection
rlogin Open an rlogin
connection
show Show running system
information
slip Start Serial-line IP (SLIP)
systat Display information
about terminal lines
telnet Open a telnet
connection
terminal Set terminal line
parameters
--More--
```

privileged EXEC mode دستورات	
Exec commands: access-enable Create a temporary Access-List entry access-profile Apply user-profile to interface access-template Create a temporary Access-List entry bfe For manual emergency modes setting clear Reset functions clock Manage the system clock configure Enter configuration mode connect Open a terminal connection copy Copy configuration or image data debug Debugging functions (see also 'undebug') disable Turn off privileged commands disconnect Disconnect an existing network connection enable Turn on privileged commands erase Erase flash or configuration memory exit Exit from the EXEC help Description of the interactive help system lock Lock the terminal login Log in as a particular	**#Router?**

```
user
logout Exit from the EXEC
mrinfo Request neighbor and
version information from a
multicast router
mstat Show statistics after
multiple multicast traceroutes
mtrace Trace reverse multicast
path from destination to
source
name-connection Name an
existing network connection
no Disable debugging
functions
pad Open a X.29 PAD
connection
ping Send echo messages
ppp Start IETF Point-to-Point
Protocol (PPP)
--More--
```

برای آشنائی با نحوه استفاده از بخش رابط کاربر روتر ، یک نمونه مثال (**تنظیم ساعت روتر**) را با هم دنبال می نمائیم :

- مرحله اول : تایپ علامت "?" به منظور آگاهی از دستورات موجود (استفاده از دستور clock)
- مرحله دوم : بررسی گرامر دستور و این که زمان را می بایست با چه فرمتی وارد نمود .
- مرحله سوم : پس از تایپ ساعت، دقیقه و ثانیه، به شما اعلام می گردد که به اطلاعات بیشتری نیاز می باشد (روز ، ماه ، سال).

- مرحله چهارم : با فشردن کلیدهای ctrl-P و یا (کلید up arrow) دستور تایپ شده قبلی تکرار و با اضافه نمودن علامت سوال به انتهای آن ، وضعیت آرگومان های اضافی آن مشخص می گردد.
- مرحله پنجم :با مشاهده علامت "^" و پاسخ سیستم ، شاهد بروز یک خطاء خواهیم بود . محل علامت "^" ، مکان احتمالی بروز خطاء را نشان می دهد. برای تایپ صحیح دستور ، مجددا" دستور را تا محلی که علامت "^" مشخص نموده تایپ کرده و سپس از علامت "?" برای آگاهی از گرامر مربوطه استفاده می نمائیم .
- مرحله ششم : پس از درج ساعت ، دقیقه و ثانیه بر اساس فرمت درخواستی ، در ادامه سال را نیز با توجه به فرمت مورد نظر وارد می نمائیم .

تنظیم زمان روتر

```
Router Con0 is now available

Press RETURN to get started.

Router>enable
Router#cl?
clear clock

Router#clock ?
set Set the time and date

Router#clock set ?
hh:mm:ss Current Time

Router#clock set 13:22:00 ?
<1-31> Day of the month
MONTH Month of the year

Router#clock set 13:22:00 17 october ?
<1999-2035> Year

Router#clock set 13:22:00 17 october 2005
Router#
```

دستورات اضافی ویرایش

بخش رابط کاربر شامل یک mode اضافی ویرایش است که با تعریف مجموعه ای از کلیدها ، امکان ویرایش یک دستور را در اختیار کاربر قرار می دهد. mode فوق ، به صورت پیش فرض فعال می گردد و در صورت تمایل می توان آن را با استفاده از دستور terminal no editing در privileged EXEC mode غیرفعال نمود. در این mode ، از Scrolling افقی در مواردی که طول یک دستور از یک خط تجاوز می نماید، استفاده می گردد. در چنین مواردی و زمانی که cursor به منتهی الیه سمت راست می رسد ، خط دستور به اندازه ده حرف به سمت چپ شیفت پیدا نموده و اولین ده حرف تایپ شده نمایش داده نخواهند شد. وجود علامت "$" در ابتدای یک دستور نشاندهنده این موضوع است که خط به سمت چپ scroll نموده است.

استفاده از سوابق دستورات تایپ شده

بخش رابط کاربر روتر به منظور استفاده مجدد از دستورات تایپ شده ، آنان را در یک بافر و با ظرفیت محدود نگهداری می نماید (سوابق و یا تاریخچه دستورات). با استفاده از امکانات موجود می توان عملیات زیر را در ارتباط با سوابق دستورات انجام داد:

- تنظیم و مشخص نمودن اندازه بافر سوابق
- فراخوانی مجدد دستورات
- غیرفعال نمودن ویژگی "سوابق دستورات "

سوابق دستورات به صورت پیش فرض فعال می گردد و قادر به ذخیره حداکثر ده خط دستور در بافر مربوطه می باشد. برای تغییر تعداد دستوراتی که می توان آنان را در لیست سوابق نگهداری نمود، از دستور terminal history size و یا history size

استفاده می گردد . حداکثر ۲۵۶ دستور را می توان در لیست سوابق نگهداری نمود. برای دستیابی به دستورات تایپ شده ، از کلیدهای Ctrl-P و یا کلید arrow Up (حرکت به سمت ابتدای لیست) و کلیدهای Ctrl-N و یا down arrow (حرکت به سمت پائین لیست) استفاده می گردد.

شبکه های بدون کابل

شبکه های بدون کابل یکی از چندین روش موجود به منظور اتصال چند کامپیوتر بیکدیگر و ایجاد یک شبکه کامپیوتری است . در شبکه های فوق برای ارسال اطلاعات بین کامپیوترهای موجود در شبکه از امواج رادیوئی استفاده می شود.

مبانی شبکه های بدون کابل

تکنولوژی شبکه های بدون کابل از ایده" **ضرورتی به کابل ها ی جدید نمی باشد**"، استفاده می نمایند. در این نوع شبکه ها، تمام کامپیوترها با استفاده از سیگنال هائی رادیوئی اقدام به انتشار اطلاعات مورد نظر برای یکدیگر می نمایند. این نوع شبکه ها دارای ساختاری ساده بوده و براحتی می توان یک کامپیوتر متصل به این نوع از شبکه ها را مکان های دیگر استقرار و کماکن از امکانات شبکه بهره مند گردید مثلا" در صورتی که این نوع شبکه ها را در یک فضای کوچک نظیر یک ساختمان اداری ایجاد کرده باشیم و دارای یک کامپیوتر laptop باشیم که از کارت شبکه مخصوص بدون کابل استفاده می نماید، در هر مکانی از اداره مورد نظر که مستقر شده باشیم با استفاده از Laptop می توان بسادگی به شبکه متصل و از امکانات مربوطه استفاده کرد.

شبکه های کامپیوتری از نقطه نظر نوع خدمات وسرویس دهی به دو گروه: نظیر به نظیر و سرویس گیرنده / سرویس دهنده نقسیم می گردند. در شبکه های نظیر به نظیر هر کامپیوتر قادر به ایفای وظیفه در دو نقش سرویس گیرنده و سرویس دهنده در هر لحظه است. در شبکه های سرویس گیرنده / سرویس دهنده، هر کامپیوتر صرفا" می تواند یک نقش را بازی نماید. (سرویس دهنده **یا** سرویس گیرنده). در شبکه های بدون کابل که بصورت نظیر به نظیر پیاده سازی می گردنند، هر کامپیوتر قادر به ارتباط مستقیم با هر یک از کامپیوترهای موجود در شبکه است. برخی دیگر از شبکه های بدون کابل بصورت سرویس گیرنده / سرویس دهنده، پیاده سازی می گردند. این نوع شبکه ها دارای یک Access point می باشند.

دستگاه فوق یک کنترل کننده کابلی بوده و قادر به دریافت و ارسال اطلاعات به آداپتورهای بدون کابل (کارت های شبکه بدون کابل) نصب شده در هر یک از کامپیوترها می باشند.

چهار نوع متفاوت از شبکه های بدون کابل وجود دارد (از کند و ارزان تا سریع وگران)

- BlueTooth
- IrDA
- HomeRF(SWAP)
- WECA(Wi-Fi)

شبکه های Bluetooth در حال حاضر عمومیت نداشته و بنظر قادر به پاسخگوئی به کاربران برای شبکه ها ی با سرعت بالا نمی باشند. IrDA(Infrared Data Association) استانداردی به منظور ارتباط دستگاههائی است که از سیگنال ها ی نوری مادون قرمز استفاده می نمایند. استاندارد فوق نحوه عملیات کنترل از راه دور، (تولید شده توسط یک تولید کننده خاص) و یک دستگاه راه دور (تولید شده توسط تولید کننده دیگر) را تبیین می کند. دستگاههای IrDA از نورمادون قرمز استفاده می نمایند.

قبل از بررسی مدل های SWAP و Wi-Fi لازم است که در ابتدا با استاندارد اولیه ای که دو مد ل فوق بر اساس آنها ارائه شده اند ، بیشتر آشنا شویم. اولین مشخصات شبکه های اترنت بدو ن کابل با نام IEEE 802.11 توسط موسسه IEEE عرضه گردید. در استاندارد فوق دو روش به منظور ارتباط بین دستگاهها با سرعت دو مگابیت در ثانیه مطرح شد. دو روش فوق بشرح زیر می باشند:

- DSSS(Direct-sequence spread spectrum)
- FHSS(Frequency-hopping spread spectrum)

دو روش فوق از تکنولوژی FSK(Frequency-shift keying) استفاده می نمایند. همچنین دو روش فوق از امواج رادیوئی Spread-spectrum در محدوده ٢/٤ گیگاهرتز استفاده می نمایند.

Spread Spectrum ، بدین معنی است که داده مورد نظر برای ارسال به بخش های کوچکتر تقسیم و هر یک از آنها با استفاده از فرکانس های گسسته قابل دستیابی در هر زمان ، ارسال خواهند شد. دستگاههائی که از DSSS استفاده می نمایند، هر بایت داده را به چندین بخش مجزا تقسیم و آنها را بصورت همزمان با استفاده از فرکانس های متفاوت، ارسال می دارند.

DSSS از پهنای باند بسیار بالائی استفاده می نماید (تقریبا" ۲۲ مگاهرتز) دستگاههائی که از FHSS استفاده می نمایند، دریک زمان پیوسته کوتاه ، اقدام به ارسال داده کرده و با شیفت دادن فرکانس (hop) بخش دیگری از اطلاعات را ارسال می نمایند. با توجه به اینکه هر یک از دستگاههای FHSS که با یکدیگر مرتبط می گردند، بر اساس فرکانس مربوطه ای که می بایست Hop نمایند و از هر فرکانس در یک بازه زمانی بسیار کوتاه استفاده می نمایند(حدودا" ٤۰۰میلی ثانیه)، بنابراین می توان از چندین شبکهFHSS در یک محیط استفاده کرد(بدون اثرات جانبی). دستگاههای FHSS صرفا" دارای پهنای باند یک مگاهرتز و یا کمتر می باشند.

HomeRF و SWAP

HomeRF ، اتحادیه ای است که استانداری با نام SWAP (Shared Wireless Access protocol) را ایجاد نموده است. SWAP دارای شش کانال صوتی متفاوت بر اساس استاندارد DECT و ۸۰۲،۱۱ است. دستگاههای SWAP در هر ثانیه ۵۰ hop ایجاد و در هر ثانیه قادر به ارسال یک مگابیت در ثانیه می باشند. در برخی از مدل ها میزان ارسال اطلاعات تا دو مگابیت در ثانیه هم می رسد. ، توانائی فوق ارتباط مستقیم به تعداد اینترفیس های موجود در مجیط عملیاتی دارد. مزایای SWAP عبارتند از:

- قیمت مناسب
- نصب آسان
- به کابل های اضافه نیاز نخواهد بود

- دارای Access point نیست
- دارای شش کانال صوتی دو طرفه و یک کانال داده است
- امکان استفاده از ۱۲۷ دستگاه در هر شبکه وجود دارد.
- امکان داشتن چندین شبکه در یک محل را فراهم می نماید.
- امکان رمزنگاری اطلاعات به منظور ایمن سازی داده ها وجود دارد.

برخی از اشکالات SWAP عبارتند از:

- دارای سرعت بالا نیست (در حالت عادی یک مگابیت در ثانیه)
- دارای دامنه محدودی است (۷۵ تا ۱۲۵ فوت / ۲۳ تا ۳۸ متر)
- با دستگاههای FHSS سازگار نیست.
- دستگاههای دارای فلز و یا وجود دیوار می تواند باعث افت ارتباطات شود.
- استفاده در شبکه های کابلی مشکل است.

تراتسیور بدون کابل واقعی بهمراه یک آنتن کوچک در یک کارت ISA ، PCI و یا PCMCIA ایجاد(ساخته) می گردد. در صورتی که از یک کامپیوتر Laptop استفاده می شود، کارت PCMCIA بصورت مستقیم به یکی از اسلات های PCMCIA متصل خواهد شد. در کامپیوترهای شخصی، می بایست از یک کارت اختصاصی ISA ، کارت HomeRF PCI و یا یک کارت PCMCIA بهمراه یک آداپتور مخصوص، استفاده کرد. با توجه به ضرورت استفاده از کارت های اختصاصی، صرفا" کامپیوترها را می توان در یک شبکه SWAP استفاده کرد. چاپگرها و سایر وسائل جانبی می بایست مستقیما" به یک کامپیوتر متصل و توسط کامپیوتر مورد نظر به عنوان یک منبع اشتراکی مورد استفاده قرار گیرند.

اکثر شبکه های SWAP بصورت "نظیر به نظیر" می باشند. برخی از تولیدکنندگان اخیرا" به منظور افزایش دامنه تاثیر پذیری در شبکه های بدون کابل، Access point هائی را به بازار عرضه نموده اند. شبکه های HomeRf نسبت به سایر شبکه های بدون کابل، دارای قیمت مناسب تری می باشند.

WECA و Wi-Fi

WECA(Alliance Wireless Ethernet Compatibility) رویکرد جدیدی را نسبت به HomeRF ارائه نموده است. Wi-Fi ، استانداردی است که به تمام تولیدکنندگان برای تولید محصولات مبتی بر استاندارد IEEE ۸۰۲،۱۱ تاکید می نماید. مشخصات فوق FHSS را حذف و تاکید بر استفاده از DSSS دارد. (بدلیل ظرفیت بالا در نرخ انتقال اطلاعات). بر اساس IEEE 802.11b ، هر دستگاه قادر به برقراری ارتباط با سرعت یازده مگابیت در ثانیه است. در صورتی که سرعت فوق پاسخگو نباشد ، بتدریج سرعت به ۵/۵ مگابیت در ثانیه، دو مگابیت در ثانیه و نهایتا" به یک مگابیت در ثانیه تنزل پیدا خواهد کرد. بدین ترتیب شبکه از صلابت و اعتماد بیشتری برخوردار خواهد بود.

مزایای Wi-Fi عبارتند از :

- سرعت بالا (یازده مگابیت در ثانیه)
- قابل اعتماد
- دارای دامنه بالائی می باشند (۱،۰۰۰ فوت یا ۳۰۵ متر در قضای باز و ۲۵۰ تا ٤۰۰ فوت / ٧٦ تا ۱۲۲ متر در فضای بسته)
- با شبکه های کابلی بسادگی ترکیب می گرد.
- با دستگاههای DSSS 802.11 (اولیه) سازگار است.

برخی از اشکالات Wi-Fi عبارتند از:

- گران قیمت می باشند.
- پیکربندی و تنظیمات آن مشکل است.
- نوسانات سرعت زیاد است.

Wi-Fi سرعت شبکه های اترنت را بدون استفاده از کابل در اختیار قرار می دهد. کارت های سازگار با Wi-Fi به منظور استفاده در شبکه های " نظیر به نظیر " وجود دارد، ولی معمولا" Wi-Fi به Access Point نیاز خواهد داشت. اغلب Access point ها

دارای یک اینترفیس به منظور اتصال به یک شبکه کابلی اترنت نیز می باشند. اکثر ترانسیورهای Wi-Fi بصورت کارت های PCMCIA عرضه شده اند. برخی از تولیدکنندگان کارت های PCI و یا ISA را نیز عرضه نموده اند.

انواع شبکه های Wireless

امروزه از شبکه های بدون کابل (Wireless) در ابعاد متفاوت و با اهداف مختلف، استفاده می شود. برقراری یک تماس از طریق دستگاه موبایل، دریافت یک پیام بر روی دستگاه pager و دریافت نامه های الکترونیکی از طریق یک دستگاه PDA، نمونه هائی از کاربرد این نوع از شبکه ها می باشند. در تمامی موارد فوق، داده و یا صوت از طریق یک شبکه بدون کابل در اختیار سرویس گیرندگان قرار می گیرد. در صورتی که یک کاربر، برنامه و یا سازمان تمایل به ایجاد پتاسیل قابلیت حمل داده را داشته باشد، می تواند از شبکه های بدون کابل استفاده نماید. یک شبکه بدون کابل علاوه بر صرفه جوئی در زمان و هزینه کابل کشی، امکان بروز مسائل مرتبط با یک شبکه کابلی را نخواهد داشت.

از شبکه های بدون کابل می توان در مکان عمومی، کتابخانه ها، هتل ها، رستوران ها و مدارس استفاده نمود. در تمامی مکان های فوق، می توان امکان دستیابی به اینترنت را نیز فراهم نمود. یکی از چالش های اصلی اینترنت بدون کابل، به کیفیت سرویس (QoS) ارائه شده برمی گردد. در صورتی که به هر دلیلی بر روی خط پارازیت ایجاد گردد، ممکن است ارتباط ایجاد شده قطع و یا امکان استفاده مطلوب از آن وجود نداشته باشد.

انواع شبکه های wireless

- **WLANS: Wireless Local Area Networks** . شبکه های فوق، امکان دستیابی کاربران ساکن در یک منطقه محدود نظیر محوطه یک دانشگاه و یا کتابخانه را به شبکه و یا اینترنت، فراهم می نماید.

- **WPANS: Wireless Personal Area Networks** . در شبکه های فوق، امکان ارتباط بین دستگاههای شخصی (نظیر laptop) در یک ناحیه محدود (حدود ۹۱٤ سانتی متر) فراهم می گردد. در این نوع شبکه ها از دو تکنولوژی متداول Infra Red (IR) و (Bluetooth (IEEE 802.15 ، استفاده می گردد.
- **WMANS: Wireless Metropolitan Area Networks** . در شبکه های فوق، امکان ارتباط بین چندین شبکه موجود در یک شهر بزرگ فراهم می گردد. از شبکه های فوق، اغلب به عنوان شبکه های backup کابلی (مسی ،فیبر نوری) استفاده می گردد.
- **WWANS: Wireless Wide Area Networks** . در شبکه های فوق، امکان ارتباط بین شهرها و یا حتی کشورها و از طریق سیستم های ماهواره ای متفاوت فراهم می گردد. شبکه های فوق به سیستم های G۲ (نسل دوم) معروف شده اند.

امنیت

برای پیاده سازی امنیـت در شبکه های بدون کابل از سه روش متفاوت استفاده می شود:

- **WEP : Wired Equivalent Privacy** . در روش فوق، هدف توقف ره گیری سیگنال های فرکانس رادیوئی توسط کاربران غیر مجاز بوده و برای شبکه های کوچک مناسب است. علت این امر به عدم وجود پروتکل خاصی به منظور مدیریت "کلید " بر می گردد. هر "کلید " می بایست به صورت دستی برای سرویس گیرندگان تعریف گردد. بدیهی است در صورت بزرگ بودن شبکه، فرآیند فوق از جمله عملیات وقت گیر برای هر مدیر شبکه خواهد بود. WEP، مبتنی بر الگوریتم رمزنگاری RC4 است که توسط RSA Data System ارائه شده است. در این رابطه تمامی سرویس گیرندگان و Point Aceess ها بگونه ای

پیکربندی می گردند که از یک کلید مشابه برای رمزنگاری و رمزگشائی استفاده نمایند.

- **SSID: Service Set Identifier**. روش فوق به منزله یک "رمزعبور" بوده که امکان تقسیم یک شبکه WLAN به چندین شبکه متفاوت دیگر که هر یک دارای یک شناسه منحصر بفرد می باشند را فراهم می نماید . شناسه های فوق، می بایست برای هر access point تعریف گردند. یک کامپیوتر سرویس گیرنده به منظور دستیابی به هر شبکه، می بایست بگونه ای پکربندی گردد که دارای شناسه SSID مربوط به شبکه مورد نظر باشد. در صورتی که شناسه کامپیوتر سرویس گیرنده با شناسه شبکه مورد نظر مطابقت نماید، امکان دستیابی به شبکه برای سرویس گیرنده فراهم می گردد.
- **فیلترینگ آدرس های (MAC) Control Media Access** : در روش فوق، لیستی از آدرس های MAC مربوط به کامپیوترهای سرویس گیرنده، برای یک Point Access تعریف می گردد. بدین ترتیب، صرفا" به کامپیوترهای فوق امکان دستیابی داده می شود. زمانی که یک کامپیوتر درخواستی را ایجاد می نماید، آدرس MAC آن با آدرس MAC موجود در Access Point مقایسه شده و در صورت مطابقت آنان با یکدیگر، امکان دستیابی فراهم می گردد . این روش از لحاظ امنیتی شرایط مناسبی را ارائه می نماید، ولی با توجه به این که می بایست هر یک از آدرس های MAC را برای هر Access point تعریف نمود، زمان زیادی صرف خواهد شد. استفاده از روش فوق، صرفا" در شبکه های کوچک بدون کابل پیشنهاد می گردد.

پیکربندی یک شبکه Wireless

سخت افزار مورد نیاز به منظور پیکربندی یک شبکه بدون کابل به ابعاد شبکه مورد نظر بستگی دارد . علیرغم موضوع فوق ، در این نوع شبکه ها اغلب و شاید هم قطعا" به یک access point و یک اینترفیس کارت شبکه نیاز خواهد بود . در صورتی که قصد ایجاد یک شبکه موقت بین دو کامپیوتر را داشته باشید ، صرفا" به دو کارت شبـــکه بدون کابل نیاز خواهید داشت.

Access Point چیست ؟

سخت افزار فوق ، به عنوان یک پل ارتباطی بین شبکه های کابلی و دستگاههای بدون کابل عمل می نماید . با استفاده از سخت افزار فوق، امکان ارتباط چندین دستگاه به منظور دستیابی به شبکه فراهم می گردد.point access می تواند دارای عملکردی مشابه یک روتر نیز باشد. در چنین مواردی انتقال اطلاعات در محدوده وسیعتری انجام شده و داده از یک point access به access point دیگر ارسال می گردد.

یک نمونه دستگاه access point

کارت شبکه بدون کابل

هر یک از دستگاههای موجود بر روی یک شبکه بدون کابل ، به یک کارت شبکه بدون کابل نیاز خواهند داشت . یک کامپیوتر Laptop ، عموما" دارای یک اسلات PCMCIA است که کارت شبکه درون آن قرار می گیرد . کامپیوترهای شخصی نیز به یک کارت شبکه داخلی که معمولا" دارای یک آنتن کوچک و یا آنتن خارجی است، نیاز

خواهند داشت .آنتن های فوق بر روی اغلب دستگاهها ،اختیاری بوده و افزایش سیگنال بر روی کارت را بدنبال خواهد داشت.

یک نمونه کارت شبکه بدون کابل

پیکربندی یک شبکه بدون کابل

به منظور پیکربندی یک شبکه بدون کابل از دو روش متفاوت استفاده می گردد:

- روش **Infrastructure** : به این نوع شبکه ها، hosted و یا managed نیز گفته می شود . در این روش از یک و یا چندین access point (موسوم به gateway و یا روترهای بدون کابل) که به یک شبکه موجود متصل می گردند ، استفاده می شود . بدین ترتیب دستگاههای بدون کابل، امکان استفاده از منابع موجود بر روی شبکه نظیر چاپگر و یا اینترنت را بدست می آورند.
- روش **Ad-Hoc** : به این نوع شبکه ها ، unmanaged و یا peer to peer نیز گفته می شود. در روش فوق هر یک از دستگاهها مستقیما" به یکدیگر متصل می گردند.مثلا" یک شخص با دارا بودن یک دستگاه کامپیوتر laptop مستقر در محوطه منزل خود می تواتند با کامپیوتر شخصی موجود در منزل خود به منظور دستیابی به اینترنت، ارتباط برقرار نماید.

پس از تهیه تجهیزات سخت افزاری مورد نیاز به منظور ایجاد یک شبکه بدون کابل، در ادامه می بایست تمامی تجهیزات تهیه شده را با هدف ایجاد و سازماندهی یک شبکه به یکدیگر متصل تا امکان ارتباط بین آنان فراهم گردد. قبل از نصب و پیکربندی یک شبکه بدون کابل، لازم است به موارد زیر دقت نمائید:

- تهیه درایورهای مربوطه از فروشنده سخت افزار و کسب آخرین اطلاعات مورد نیاز
- فاصله بین دو کامپیوتر می بایست کمتر از یکصد متر باشد.
- هر یک از کامپیوترهای موجود می بایست بر روی یک طبقه مشابه باشند.
- استفاده از تجهیزات سخت افزاری مربوط به یک تولید کننده، دارای مزایا و معایبی است. در این رابطه پیشنهاد می گردد لیستی از ویژگی های هر یک از سخت افزارهای مورد نیاز عرضه شده توسط تولید کنندگان متعدد تهیه شود تا امکان مقایسه و اخذ تصمیم مناسب، فراهم گردد.

مراحل لازم به منظور نصب یک شبکه (فرضیات : ما دارای یک شبکه کابلی موجود هستیم و قصد پیاده سازی یک شبکه بدون کابل به منظور ارتباط دستگاههای بدون کابل به آن را داریم):

- اتصال point access به برق و سوکت مربوط به شبکه اترنت
- پیکربندی access point (معمولا" از طریق یک مرورگر وب) تا امکان مشاهده آن توسط شبکه موجود فراهم گردد. نحوه پیکربندی point access بستگی به نوع آن دارد.
- پیکربندی مناسب کامپیوترهای سرویس گیرنده به منظور ارتباط با access point (در صورتی که تمامی سخت افزارهای شبکه بدون کابل از یک تولید کننده تهیه شده باشند ، عموما" با تنظیمات پیش فرض هم می توان شبکه را فعال نمود . به هر حال پیشنهاد می گردد همواره به راهنمای سخت افزار تهیه شده به منظور پیکربندی بهینه آنان ، مراجعه گردد).

پهنای باند و میزان تاخیر

پهنای باند از جمله واژه های متداول در دنیای شبکه های کامپیوتری است که به نرخ انتقال داده توسط یک اتصال شبکه و یا یک اینترفیس، اشاره می نماید. این واژه از رشته مهندسی برق اقتباس شده است. در این شاخه از علوم، پهنای باند نشان دهنده مجموع فاصله و یا محدوده بین بالاترین و پائین ترین سیگنال بر روی کانال های مخابرانی (باند)، است. به منظور سنجش اندازه پهنای باند از واحد " تعداد بایت درثانیه " و یا bps استفاده می شود.

پهنای باند تنها عامل تعیین کننده سرعت یک شبکه از زاویه کاربران نبوده و یکی دیگر از عناصر تاثیرگذار، "میزان تاخیر" در یک شبکه است که می تواند برنامه های متعددی را که بر روی شبکه اجراء می گردند، تحت تاثیر قرار دهد.

پهنای باند چیست ؟

تولید کنندگان تجهیزات سخت افزاری شبکه در زمان ارائه محصولات خود تبلیغات زیادی را در ارتباط با پهنای باند، انجام می دهند. اکثر کاربران اینترنت نسبت به میزان پهنای باند مودم خود و یا سرویس اینترنت braodband دارای آگاهی لازم می باشند. پهنای باند، ظرفیت اتصال ایجاد شده را مشخص نموده و بدیهی است که هر اندازه ظرفیت فوق بیشتر باشد، امکان دستیابی به منابع شبکه با سرعت بیشتری فراهم می گردد. پهنای باند، ظرفیت تئوری و یا عملی یک اتصال شبکه و یا یک اینترفیس را مشخص نموده که در عمل ممکن است با یکدیگر متفاوت باشند. مثلا" یک مودم V.90 پهنای باندی معادل ٥٦ kbps را در حالت سقف پهنای باند حمایت می نماید ولی با توجه به محدودیت های خطوط تلفن و سایر عوامل موجود، عملا" امکان رسیدن به محدوده فوق وجود نخواهد داشت . یک شبکه اترنت سریع نیز از لحاظ تئوری قادر به

حمایت پهنای باندی معادل Mbps۱۰۰ است، ولی عملا" این وضعیت در عمل محقق نخواهد شد (تفاوت ظرفیت تئوری پهنای باند با ظرفیت واقعی).

پهنای باند بالا و broadband

در برخی موارد واژه های "پهنای باند بالا" و " braodband " به جای یکدیگر استفاده می گردند. کارشناسان شبکه در برخی موارد از واژه "پهنای باند بالا " به منظور مشخص نمودن سرعت بالای اتصال به اینترنت استفاده می نمایند . در این رابطه تعاریف متفاوتی وجود دارد . این نوع اتصالات، پهنای باندی بین Kbps٦٤ تا kbps۳۰۰ و یا بیشتر را ارائه می نـمایند. پهنای باند بالا با broadband متفاوت است.

broadband ، نشاندهنده روش استفاده شده به منظور ایجاد یک ارتباط است در صورتی که پهنای باند ، نرخ انتقال داده از طریق محیط انتقال را نشان می دهد.

اندازه گیری پهنای باند شبکه

به منظور اندازه گیری پهنای باند اتصال شبکه می توان از ابزارهای متعددی استفاده نمود . برای اندازه گیری پهنای باند در شبکه های محلی (LAN) ، از برنامه هائی نظیر netpref و ttcp ، استفاده می گردد. در زمان اتصال به اینترنت و به منظور تست پهنای باند می توان از برنامه های متعددی استفاده نمود . تعداد زیادی از برنامه های فوق را می توان با مراجعه به صفحات وب عمومی استفاده نمود . صرفنظر از نوع نرم افزاری که از آن به منظور اندازه گیری پهنای باند استفاده می گردد، پهنای باند دارای محدوده بسیار متغیری است که اندازه گیری دقیق آن امری مشکل است.

تاخیر

پهنای باندصرفا" یکی از عناصرتاثیرگذار درسرعت یک شبکه است.

تاخیر(Latency) که نشاندهنده میزان تاخیر در پردازش داده در شبکه است، یکی دیگر از عناصر مهم در ارزیابی کارآئی و سرعت یک شبکه است که دارای ارتباطی نزدیک با پهنای باند می باشد. از لحاظ تئوری سقف پهنای باند ثابت

است. پهنای باند واقعی متغیر بوده و می تواند عامل بروز تاخیر در یک شبکه گردد. وجود تاخیر زیاد در پردازش داده در شبکه و در یک محدوده زمانی کوتاه می تواند باعث بروز یک بحران در شبکه شده و پیامد آن پیشگیری از حرکت داده بر روی محیط انتقال و کاهش استفاده موثر از پهنای باند باشد.

تاخیر و سرویس اینترنت ماهواره ای

دستیابی به اینترنت با استفاده از ماهواره به خوبی تفاوت بین پهنای باند و تاخیر را نشان می دهد . ارتباطات مبتنی بر ماهواره دارای پهنای باند و تاخیر بالائی می باشند. مثلا" زمانی که کاربری درخواست یک صفحه وب را می نمائید، مدت زمانی که بطول می انجامد تا صفحه درحافظه مستقر گردد با این که کوتاه بنظر می آید ولی کاملا" ملموس است. تاخیر فوق به دلیل تاخیر انتشار است. علاوه بر تاخیر انتشار، یک شبکه ممکن است با نوع های دیگری از تاخیر مواجه گردد. تاخیر انتقال (مرتبط با خصایص فیزیکی محیط انتقال) و تاخیر پردازش (ارسال درخواست از طریق سرویس دهندگان پروکسی و یا ایجاد hops بر روی اینترنت) دو نمونه متداول در این زمینه می باشند.

اندازه گیری تاخیر در یک شبکه

از ابزارهای شبکه ای متعددی نظیر ping و traceroute می توان به منظور اندازه گیری میزان تاخیر در یک شبکه استفاده نمود . برنامه های فوق فاصله زمانی بین ارسال یک بسته اطلاعاتی از مبداء به مقصد و برگشت آن را محاسبه می نمایند. به زمان فوق round-trip ، گفته می شود. round-trip تنها روش موجود به منظور تشخیص و یا بدست آوردن میزان تاخیر در یک شبکه نبوده و در این رابطه می توان از برنامه های متعددی استفاده نمود.

پهنای باند و تاخیر دو عنصر تاثیر گذار در کارائی یک شبکه می باشند .معمولا" از واژه QoS (Quality of Service) به منظور نشان دادن وضعیت کارآئی یک شبکه استفاده می گردد که در آن دو شاخص مهم پهنای باند و تاخیر مورد توجه قرار می گیرد.

انواع کابل

امروزه از کابل های مختلفی در شبکه ها استفاده می گردد. نوع و سیستم کابل کشی استفاده شده در یک شبکه بسیار حائز اهمیت است. در صورتی که قصد داشتن شبکه ای را داریم که دارای حداقل مشکلات باشد و بتواند با استفاده مفید از پهنای باند به درستی خدمات خود را در اختیار کاربران قرار دهد، می بایست از یک سیستم کابلینگ مناسب، استفاده گردد. در زمان طراحی یک شبکه می بایست با رعایت مجموعه قوانین موجود در خصوص سیستم کابلینگ، شبکه ای با حداقل مشکلات را طراحی نمود.با این که استفاده از شبکه های بدون کابل نیز در ابعاد وسیعی گسترش یافته است، ولی هنوز بیش از ۹۵ درصد سازمان ها و موسسات از سیستم های شبکه ای مبتنی بر کابل، استفاده می نمایند.

ایده های اولیه

ایده مبادله اطلاعات به صورت دیجیتال، تفکری جدید در عصر حاضر محسوب می گردد. درسال ۱۸٤٤ فردی با نام"ساموئل مورس"، یک پیام را از **Washington D.C** به **Baltimore** و با استفاده از اختراع جدید خود (تلگراف)، ارسال نمود. با این که از آن موقع زمانی زیادی گذشته است و ما امروزه شاهد شبکه های کامپیوتری بزرگ و در عین حال پیچیده ای می باشیم ولی می توان ادعا نمود که اصول کار ، همان اصول و مفاهیم گذشته است.

کدهای مورس، نوع خاصی از سیستم باینری می باشند که از نقطه و خط فاصله با ترکیبات متفاوت به منظور ارائه حروف و اعداد ، استفاده می نماید. شبکه های مدرن داده از یک و صفر ، استفاده می نمایند . بزگترین تفاوت موجود بین سیستم های مدرن مبادله اطلاعات و سیستم پیشنهادی "مورس "، سرعت مبادله اطلاعات در آنان

است.تلگراف های اواسط قرن ۱۹ ، قادر به ارسال چهار تا پنج نقطه و یا خط فاصله در هر ثانیه بودند ، در حالی که هم اینک کامپیوترها با سرعتی معادل یک گیگابیت در ثانیه با یکدیگر ارتباط برقرار می نمایند (ارسال ۱،۰۰۰،۰۰۰،۰۰۰ صفر و یا یک در هر ثانیه). تلگراف و تله تایپ رایتر ، پیشگام مبادله داده می باشند . در طی سی و پنج سال اخیر همه چیز با سرعت بالا و غیرقابل تصوری تغییر نموده است. ضرورت ارتباط کامپیوترها با یکدیگر و با سرعت بالا ، مهمترین علل پیاده سازی تجهیزات شبکه ای سریع، کابل هائی با مشخصات بالا و سخت افزارهای ارتباطی پیشرفته است.

پیاده سازی تکنولوژی های جدید شبکه

اترنت در سال ۱۹۷۰ توسط شرکت زیراکس و در مرکز تحقیقات Palo Alto در کالیفرنیا پیاده سازی گردید. در سال ۱۹۷۹ شرکت های DEC و اینتل با پیوستن به زیراکس، سیستم اترنت را برای استفاده عموم، استاندارد نمودند. اولین مشخصه استاندارد در سال ۱۹۸۰ توسط سه شرکت فوق و با نام Ethernet Blue Book ارائه گردید . (استاندارد DIX).

اترنت یک سیستم ده مگابیت در ثانیه است (ده میلیون صفر و یا یک در ثانیه) که از یک کابل کواکسیال بزرگ به عنوان ستون فقرات و کابل های کواکسیال کوتاه در فواصل ۵ / ۲ متر به منظور ایستگاههای کاری استفاده می نماید . کابل کواکسیالی که به عنوان ستون فقرات استفاده می گردد ، Ethernet Thick و یا Basee5۱۰ نامیده می شود که در آن ۱۰ به سرعت انتقال اطلاعات در شبکه اشاره داشته (۱۰ مگابیت در ثانیه) و واژه Base نشاندهنده سیستم Base band است. در سیستم فوق، از تمامی پهنای باند به منظور انتقال اطلاعات استفاده می گردد. در Broad band به منظور استفاده همزمان ، پهنای باند به کانال های متعددی تقسیم می گردد.

عدد ۵ نیز شکل خلاصه شده ای برای نشان دادن حداکثر طول کابلی است که می توان استفاده نمود (در این مورد خاص ۵۰۰ متر).

موسسه IEEE در سال ۱۹۸۳ نسخه رسمی استاندارد اترنت را با نام IEEE 802.3 و در سال ۱۹۸۵ ، نسخه شماره دو را با نام IEEE 802.3a ارائه نمود . این نسخه با نام Thin Ethernet و یا Base2۱۰ معروف گردید. (حداکثر طول کابل ۱۸۵ متر می باشد و عدد ۲ نشاندهنده این موضوع است که طول کابل می تواند تا مرز ۲۰۰ متر نیز برسد)

از سال ۱۹۸۳ تاکنون ، استانداردهای متفاوتی ارائه شده است که یکی از اهداف مهم آنان ، تامین پهنای باند مناسب به منظور انتقال اطلاعات است . ما امروزه شاهد رسیدن به مرز گیگابیت در شبکه های کامپیوتری می باشیم.

کابل های (UTP) Unshielded Twisted Pair

کابل UTP یکی از متداولترین کابل های استفاده شده در شبکه های مخابراتی و کامپیوتری است . از کابل های فوق، علاوه بر شبکه های کامپیوتری در سیستم های تلفن نیز استفاده می گردد (CAT1). شش نوع کابل UTP متفاوت وجود داشته که می توان با توجه به نوع شبکه و اهداف مورد نظر از آنان استفاده نمود. کابل CAT5 ، متداولترین نوع کابل UTP محسوب می گردد.

مشخصه های کابل UTP

با توجه به مشخصه های کابل های UTP ، امکان استفاده ، نصب و توسعه سریع و آسان آنان ، فراهم می آورد . جدول زیر انواع کابل های UTP را نشان می دهد:

گروه	سرعت انتقال اطلاعات	موارد استفاده
CAT1	حداکثر تا یک مگابیت در ثانیه	سیستم های قدیمی تلفن ، ISDN و مودم
CAT2	حداکثر تا چهار مگابیت در ثانیه	شبکه های Ring Token
CAT3	حداکثر تا ده مگابیت در ثانیه	شبکه های ring Token و ۱۰-BASE T
CAT4	حداکثر تا شانزده مگابیت در ثانیه	شبکه های Ring Token
CAT5	حداکثر تا یکصد مگابیت در ثانیه	اترنت (ده مگابیت در ثانیه) ، اترنت سریع (یکصد مگابیت در ثانیه) و شبکه های Ring Token (شانزده مگابیت در ثانیه)
CAT5e	حداکثر تا یکهزار مگابیت در ثانیه	شبکه های Gigabit Ethernet
CAT6	حداکثر تا یکهزار مگابیت در ثانیه	شبکه های Gigabit Ethernet

توضیحات :

- تقسیم بندی هر یک از گروه های فوق بر اساس نوع کابل مسی و Jack انجام شده است.
- از کابل های CAT1 ، به دلیل عدم حمایت ترافیک مناسب، در شبکه های کامپیوتری استفاده نمی گردد.
- از کابل های گروه CAT2, CAT3، CAT4, CAT5 و CAT6 در شبکه ها استفاده می گردد .کابل های فوق ، قادر به حمایت از ترافیک تلفن و شبکه های کامپیوتری می باشند.

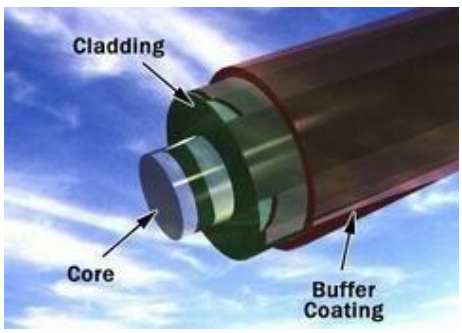
- از کابل های CAT2 در شبکه های Token Ring استفاده شده و سرعتی بالغ بر ٤ مگابیت در ثانیه را ارائه می نمایند.
- برای شبکه هائی با سرعت بالا (یکصد مگا بیت در ثانیه) از کابل های CAT5 و برای سرعت ده مگابیت در ثانیه از کابل های CAT3 استفاده می گردد.
- در کابل های CAT4, CAT3 و CAT5 از چهار زوج کابل مسی استفاده شده است. CAT5 نسبت به CAT3 دارای تعداد بیشتری پیچش در هر اینچ می باشد. بنابراین این نوع از کابل ها سرعت و مسافت بیشتر ی را حمایت می نمایند.
- از کابل های CAT3 و CAT4 در شبکه هایToken Ring استفاده می گردد.
- حداکثر مسافت در کابل های CAT3 ، یکصد متر است.
- حداکثر مسافت در کابل های CAT4 ، دویست متر است.
- کابل CAT6 با هدف استفاده در شبکه های اترنت گیگابیت طراحی شده است. در این رابطه استانداردهائی نیز وجود دارد که امکان انتقال اطلاعات گیگابیت بر روی کابل های CAT5 را فراهم می نماید(CAT5e). کابل های CAT6 مشابه کابل های CAT5 بوده ولی بین ٤ زوج کابل آنان از یک جداکننده فیزیکی به منظور کاهش پارازیت های الکترومغناطیسی استفاده شده و سرعتی بالغ بر یکهزار مگابیت در ثانیه را ارائه می نمایند.

فیبر نوری

فیبر نوری یکی از محیط های انتقال داده با سرعت بالا است. از فیبر نوری در موارد متفاوتی نظیر: شبکه های تلفن شهری و بین شهری، شبکه های کامپیوتری و اینترنت استفاده می گردد. فیبرنوری رشته ای از تارهای شیشه ای بوده که هر یک از تارها دارای ضخامتی معادل تار موی انسان را داشته و از آنان برای انتقال اطلاعات در مسافت های طولانی استفاده می شود.

مبانی فیبر نوری

فیبر نوری، رشته ای از تارهای بسیار نازک شیشه ای بوده که قطر هر یک از تارها نظیر قطر یک تار موی انسان است. تارهای فوق در کلاف هائی سازماندهی و کابل های نوری را بوجود می آورند. از فیبر نوری بمنظور ارسال سیگنال های نوری در مسافت های طولانی استفاده می شود.



یک فیبر نوری از سه بخش متفاوت تشکیل شده است:

- **هسته (Core)** . هسته نازک شیشه ای در مرکز فیبر که سیگنال های نوری در آن حرکت می نمایند.
- **روکش (Cladding)** . بخش خارجی فیبر بوده که دورتادور هسته را احاطه کرده و باعث برگشت نورمنعکس شده به هسته می گردد.
- **بافر رویه (Coating Buffer)** . روکش پلاستیکی که باعث حفاظت فیبر در مقابل رطوبت و سایر موارد آسیب پذیر، است.

صدها و هزاران نمونه از رشته های نوری فوق در دسته هائی سازماندهی شده و کابل های نوری را بوجود می آورند. هر یک از کلاف های فیبر نوری توسط یک روکش هائی با نام Jacket محافظت می گردند.

فیبر های نوری در دو گروه عمده ارائه می گردند:

- **فیبرهای تک حالته (Single-Mode)** . بمنظور ارسال یک سیگنال در هر فیبر استفاده می شود(نظیر : تلفن)
- **فیبرهای چندحالته (Multi-Mode)** . بمنظور ارسال چندین سیگنال در یک فیبر استفاده می شود(نظیر : شبکه های کامپیوتری)

فیبرهای تک حالته دارای یک هسته کوچک (تقریبا" ۹ میکرون قطر) بوده و قادر به ارسال نور لیزری مادون قرمز (طول موج از ۱۳۰۰ تا ۱۵۵۰ نانومتر) می باشند. فیبرهای چند حالته دارای هسته بزرگتر (تقریبا" ۵ / ۶۲ میکرون قطر) و قادر به ارسال نورمادون قرمز از طریق LED می باشند.

ارسال نور در فیبر نوری

فرض کنید، قصد داشته باشیم با استفاده از یک چراغ قوه یک راهروی بزرگ و مستقیم را روشن نمائیم. همزمان با روشن نمودن چراغ قوه، نور مربوطه در طول مسیر مسقیم راهرو تابانده شده و آن را روشن خواهد کرد.

با توجه به عدم وجود خم و یا پیچ در راهرو در رابطه با تابش نور چراغ قوه مشکلی وجود نداشته و چراغ قوه می تواند (با توجه به نوع آن) محدوده مورد نظر را روشن کرد. در صورتیکه راهروی فوق دارای خم و یا پیچ باشد ، با چه مشکلی برخورد خواهیم کرد؟ در این حالت می توان از یک آیینه در محل پیچ راهرو استفاده تا باعث انعکاس نور از زاویه مربوطه گردد.در صورتیکه راهروی فوق دارای پیچ های زیادی باشد، چه کار بایست کرد؟ در چنین حالتی در تمام طول مسیر دیوار راهروی مورد نظر، می بایست از آیینه استفاده کرد. بدین ترتیب نور تابانده شده توسط چراغ قوه (با یک زاویه خاص) از نقطه ای به نقطه ای دیگر حرکت کرده (جهش کرده و طول مسیر راهرو را طی خواهد کرد). عملیات فوق مشابه آنچیزی است که در فیبر نوری انجام می گیرد.

نور، در کابل فیبر نوری از طریق هسته (نظیر راهروی مثال ارائه شده) و توسط جهش های پیوسته با توجه به سطح آبکاری شده (Cladding) (مشابه دیوارهای شیشه ای مثال ارائه شده) حرکت می کند.(مجموع انعکاس داخلی). با توجه به اینکه سطح آبکاری شده ، قادر به جذب نور موجود در هسته نمی باشد، نور قادر به حرکت در مسافت های طولانی می باشد. برخی از سیگنا ل های نوری بدلیل عدم خلوص شیشه موجود ، ممکن است دچار نوعی تضعیف در طول هسته گردند. میزان تضعیف سیگنال نوری به درجه خلوص شیشه و طول موج نور انتقالی دارد. (مثلاً موج با طول ۸۵۰ نانومتر بین ٦۰ تا ۷۵ درصد در هر کیلومتر ، موج با طول ۱۳۰۰ نانومتر بین ۵۰ تا ٦۰ درصد در هر کیلومتر ، موج با طول ۱۵۵۰ نانومتر بیش از ۵۰ درصد در هر کیلومتر)

سیستم رله فیبر نوری

بمنظور آگاهی از نحوه استفاده فیبر نوری در سیستم های مخابراتی ، مثالی را دنبال خواهیم کرد که مربوط به یک فیلم سینمائی و یا مستند در رابطه با جنگ جـــهانی دوم است . در فیلم فوق دو ناوگان دریائی که بر روی سطح دریا در حال حرکت می باشند ، نیاز به برقراری ارتباط با یکدیگر در یک وضعیت کاملاً بحرانی و توفانی را دارند.

یـکی از ناوها قصد ارسال پیام برای ناو دیگر را دارد.کاپیتان ناو فوق پیامی برای یک ملوان که بر روی عرشه کشتی مستقر است، ارسال می دارد. ملوان فوق پیام دریافتی را به مجموعه ای از کدهای مورس (نقطه و فاصله) ترجمه می نماید. در ادامه ملوان مورد نظر با استفاده از یک نورافکن اقدام به ارسال پیام برای ناو دیگر می نماید. یک ملوان بر روی عرشه کشتی دوم، کدهای مورس ارسالی را مشاهده می نماید. در ادامه ملوان فوق کدهای فوق را به یک زبان خاص (مثلا" انگلیسی) تبدیل و آنها را برای کاپیتان ناو ارسال می دارد. فرض کنید فاصله دو ناو فوق از یکدیگر بسیار زیاد (هزاران مایل) بوده و بمنظور برقرای ارتباط بین آنها از یک سیستم مخابراتی مبتنی بر فیبر نوری استفاده گردد.

سیستم رله فیبر نوری از عناصر زیر تشکیل شده است:

- **فرستنده** . مسئول تولید و رمزنگاری سیگنال های نوری است.
- **فیبر نوری** مدیریت سیکنال های نوری در یک مسافت را برعهده می گیرد.
- **بازیاب نوری** . بمنظور تقویت سیگنا ل های نوری در مسافت های طولانی استفاده می گردد.
- **دریافت کننده نوری** . سیگنا ل های نوری را دریافت و رمزگشائی می نماید.

در ادامه به بررسی هر یک از عناصر فوق خواهیم پرداخت.

فرستنده

وظیفه فرستنده، مشابه نقش ملوان بر روی عرشه کشتی ناو فرستنده پیام است. فرستنده سیگنال های نوری را دریافت و دستگاه نوری را بمنظور روشن و خاموش شدن در یک دنباله مناسب (حرکت منسجم) هدایت می نماید. فرستنده، از لحاظ فیزیکی در مجاورت فیبر نوری قرار داشته و ممکن است دارای یک لنز بمنظور تمرکز نور در فیبر باشد. لیزرها دارای توان بمراتب بیشتری نسبت به LED می باشند. قیمت آنها نیز در مقایسه با LED بمراتب بیشتراست. متداولترین طول موج سیگنال های نوری، ۸۵۰ نانومتر، ۱۳۰۰ نانومتر و ۱۵۵۰ نانومتر است.

بازیاب (تقویت کننده) نوری

همانگونه که قبلا" اشاره گردید، برخی از سیگنال ها در مواردیکه مسافت ارسال اطلاعات طولانی بوده (بیش از یک کیلومتر) و یا از مواد خالص برای تهیه فیبر نوری (شیشه) استفاده نشده باشد، تضعیف و از بین خواهند رفت. در چنین مواردی و بمنظور تقویت (بالا بردن) سیگنا ل های نوری تضعیف شده از یک یا چندین " تقویت کننده نوری " استفاده می گردد. تقویت کننده نوری از فیبرهای نوری متعدد بهمراه یک روکش خاص (doping) تشکیل می گردند. بخش دوپینگ با استفاده از یک لیزر پمپ می گردد . زمانیکه سیگنال تضعیف شده به روکش دوپینگی می رسد، انرژی ماحصل از لیزر باعث می گردد که مولکول های دوپینگ شده، به لیزر تبدیل می گردند. مولکول های دوپینگ شده در ادامه باعث انعکاس یک سیگنال نوری جدید و قویتر با همان خصایص سیگنال ورودی تضعیف شده ، خواهند بود.(تقویت کننده لیزری)

دریافت کننده نوری

وظیفه دریافت کننده ، مشابه نقش ملوان بر روی عرشه کشتی ناو دریافت کننده پیام است. دستگاه فوق سیگنال های دیجیتالی نوری را اخذ و پس از رمزگشائی ، سیگنا ل های الکتریکی را برای سایر استفاده کنندگان (کامپیوتر ، تلفن و ...) ارسال می نماید. دریافت کننده بمنظور تشخیص نور از یک "فتوسل" و یا "فتودیود" استفاده می کند.

مزایای فیبر نوری

فیبر نوری در مقایسه با سیم های های مسی دارای مزایای زیر است:

- **ارزانتر**. هزینه چندین کیلومتر کابل نوری نسبت به سیم های مسی کمتر است.
- **نازک تر**. قطر فیبرهای نوری بمراتب کمتر از سیم های مسی است.
- **ظرفیت بالا** . پهنای باند فیبر نوری بمنظور ارسال اطلاعات بمراتب بیشتر از سیم مسی است.
- **تضعیف ناچیز**. تضعیف سیگنال در فیبر نوری بمراتب کمتر از سیم مسی است.

- **سیگنال های نوری** . برخلاف سیگنال های الکتریکی در یک سیم مسی ، سیگنا ل ها ی نوری در یک فیبر تاثیری بر فیبر دیگر نخواهند داشت.
- **مصرف برق پایین** . با توجه به سیگنال ها در فیبر نوری کمتر ضعیف می گردند، بنابراین می توان از فرستنده هائی با میزان برق مصرفی پایین نسبت به فرستنده های الکتریکی که از ولتاژ بالائی استفاده می نمایند، استفاده کرد.
- **سیگنال های دیجیتال** . فیبر نوری مناسب بمنظور انتقال اطلاعات دیجیتالی است.
- **غیر اشتعال زا** . با توجه به عدم وجود الکتریسیته، امکان بروز آتش سوزی وجود نخواهد داشت.
- **سبک وزن** . وزن یک کابل فیبر نوری بمراتب کمتر از کابل مسی (قابل مقایسه) است.
- **انعطاف پذیر** . با توجه به انعطاف پذیری فیبر نوری و قابلیت ارسال و دریافت نور از آنان، در موارد متفاوت نظیر دوربین های دیجیتال با موارد کاربردی خاص مانند : عکس برداری پزشکی، لوله کشی و ...استفاده می گردد.

با توجه به مزایای فراوان فیبر نوری، امروزه از این نوع کابل ها در موارد متفاوتی استفاده می شود. اکثر شبکه های کامپیوتری و یا مخابرات ازراه دور در مقیاس وسیعی از فیبر نوری استفاده می نمایند.

ایجاد کابل X-Over

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

چرا به کابل های X-over نیاز داریم ؟

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

اتصال دو کامپیوتر به یکدیگر با استفاده از یک کابل X-over

کابل CAT5 X-over

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

شماره پین های یک کابل CAT5 X-over .

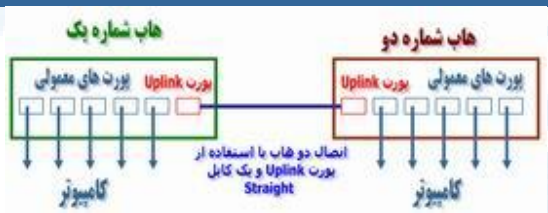
همانگونه که در شکل فوق مشاهده می گردد در کابل های X-over صرفا" از پین های شماره یک، دو، سه و شش استفاده می گردد. پین های یک و دو بمنزله یک زوج بوده و پین های سه و شش زوج دیگر را تشکیل می دهند. از پین های چهار، پنج ، هفت و هشت استفاده نمی گردد . (صرفا" از چهار پین برای ایجاد یک کابل X-over ، استفاده می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

موارد استفاده از کابل های X-over

از کابل های X-over صرفا" به منظور اتصال دو کامپیوتر استفاده نمی شود و می توان از آنان در دستگاه های متفاوتی نظیر سوئیچ و یا هاب نیز استفاده نمود. در صورتی که قصد داشته باشیم دو هاب را به یکدیگر متصل نمائیم، معمولا" از پورت uplink استفاده می گردد. پورت فوق ، بخش های tx و rx را کراس نمی نماید.

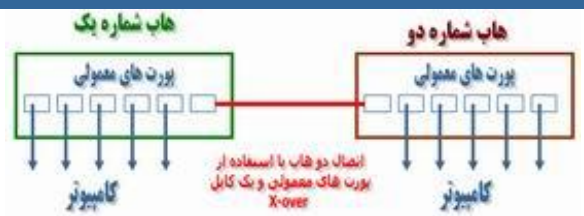
شکل زیر نحوه اتصال دو هاب به یکدیگر با استفاده از یک کابل Straight و از طریق پورت Uplink را نشان می دهد:

اتصال دو هاب با استفاده از پورت Uplink و یک کابل Straight



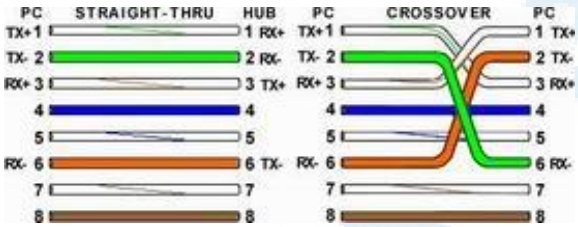
با توجه به وجود پورت uplink ، نیازی به استفاده از یک کابل x-over نخواهد بود. در صورتی که امکان استفاده از پورت uplink وجود نداشته باشد و بخواهیم دو هاب را با استفاده از پورت های معمولی به یکدیگر متصل نمائیم، می توان از یک کابل X-over استفاده نمود. شکل زیر نحوه اتصال دو هاب به یکدیگر با استفاده از یک کابل X-over را و بدون استفاده از پورت Uplink نشان می دهد:

اتصال دو هاب با استفاده از پورت معمولی و یک کابل X-over



شکل زیر تفاوت موجود بین شماره پین های یک کابل Straight و X-over را نشان می دهد :

تفاوت شماره پین های بین کابل Straight و X-over



ایجاد کابل Straight

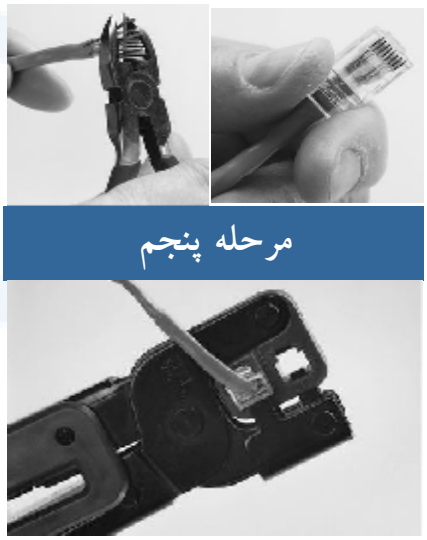
کابل کشی شبکه یکی از مراحل مهم در زمان پیاده سازی یک شبکه کامپیوتری است که می بایست با دقت،ظرافت خاص و پایبندی به اصول کابل کشی ساخت یافته، انجام شود. برای ایجاد کابل های UTP از تجهیزات زیر استفاده می گردد :

تجهیزات مورد نیاز
کانکتورهای RJ-45 کابل UTP
آچار پرس RJ-45سیم لخت کن

یکی از عوامل تاثیر گذار در پشتیبانی و نگهداری یک شبکه، نحوه کابل کشی آن است. با رعایت اصول کابل کشی ساختیافته، در صورت بروز اشکال در شبکه، تشخیص و اشکال زدائی آن با سرعتی مناسبی انجام خواهد شد.

مراحل ایجاد یک کابل : بدون هیچگونه توضیح اضافه !

مرحله اول	مرحله دوم
	
مرحله سوم	مرحله چهارم



مدل های متفاوت کابل کشی کابل های UTP

به منظور کابل کشی کابل های UTP از دو استاندارد متفاوت T-568A و T-568B استفاده می گردد. نحوه عملکرد دو مدل فوق یکسان بوده و تنها تفاوت موجود به رنگ زوج هائی است که به یکدیگر متصل می شوند. در کابل های UTP از کانکتورهای استاندارد و چهار زوج سیم بهم تابیده استفاده می گردد:

- زوج اول : آبی و سفید/ آبی
- زوج دوم : نارنجی و سفید /نارنجی
- زوج سوم : سبز و سفید/ سبز
- زوج چهارم : قهوه ای و سفید / قهوه ای

در شبکه های ۱۰/۱۰۰ Mbit از زوج های دو و سه استفاده شده و زوج های یک و چهار رزو شده می باشند. در شبکه های گیگااترنت از تمامی چهار زوج استفاده می گردد. کابل های CAT5 متداولترین نوع کابل UTP بوده که دارای انعطاف مناسب بوده و نصب آنان بسادگی انجام می شود.

ایجاد یک کابل UTP به منظور اتصال کامپیوتر به هاب (معروف به کابل های Straight)

اترنت عموما" با استفاده از هشت کابل هادی به همراه هشت پین ماژولار plugs/jacks ، داده را حمل می کند.

کانکتور استاندارد، RJ-45 نامیده شده و مشابه کانکتور استاندارد RJ-11 است که در تلفن استفاده می گردد. یک رشته کابل CAT5 شامل چهار زوج سیم بهم تابیده است که هر زوج دارای دو رشته سیم با رنگ هائی خاص است. (یک رشته رنگی و یک رشته سفید با نواری به رنگ رشته زوج مربوط). به منظور تسهیل در امر نگهداری، می بایست به اندازه ضروری سیم های بهم تابیده را از حالت پیچش خارج نمود (مثلا" حدود یک سانتیمتر). زوج های در نظر گرفته شده برای اترنت ده و یکصد مگابیت به رنگ نارنجی و سبز می باشند.

از دو زوج دیگر (رنگ قهوه ای و آبی) می توان به منظور یک خط اترنت دوم و یا اتصالات تلـفن استفاده نمود.

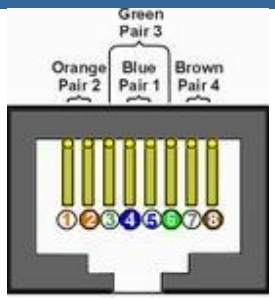
به منظور کابل کشی کابل های UTP از دو استاندارد متفاوت با نام T-568B (یا EIA) و T-568A (یا T&AT ، A۲۵۸)، استفاده می گردد. تنها تفاوت موجود بین آنان ترتیب اتصالات است.

شماره پین های استاندارد T568B

همانگونه که در جدول زیر مشاهده می گردد، شماره پین های فرد همواره سفید بوده که با یک نوار رنگی پوشش داده می شوند.

کد رنگ ها در استاندارد B۵۶۸T			
کاربرد	زوج	رنگ	شماره پین
TxData+	دوم	سفید/ نارنجی	یک
TxData-	دوم	نارنجی	دو
RecvData+	سوم	سفید / سبز	سه
	یک	آبی	چهار
	یک	سفید /آبی	پنج
RecvData-	سوم	سبز	شش
	چهارم	سفید/قهوه ای	هفت
	چهارم	قهوه ای	هشت

استاندارد B۵۶۸T

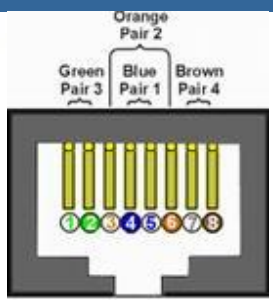


شماره پین های استاندارد T568A

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

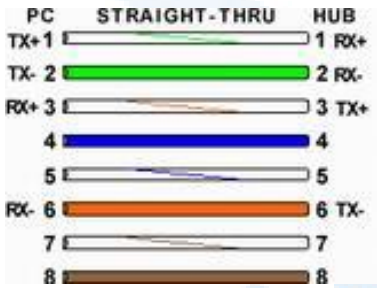
کد رنگ ها در استاندارد A۵۶۸T			
کاربرد	زوج	رنگ	شماره پین
RecvData+	سوم	سفید/ سبز	یک
RecvData-	سوم	سبز	دو
TxData+	دوم	سفید / نارنجی	سه
	یک	آبی	چهار
	یک	سفید /آبی	پنج
TxData-	دوم	نارنجی	شش
	چهارم	سفید/قهوه ای	هفت
	چهارم	قهوه ای	هشت

استاندارد A۵۶۸T



موارد استفاده

متداولترین کاربرد یک کابل straight ، اتصال بین یک کامپیوتر و هاب /سوئیچ است. در چنین مواردی، کامپیوتر مستقیما" به هاب و یا سوئیچ متصل شده که به صورت اتوماتیک و با استفاده از مداراتی خاص، کابل over cross می گردد.



شکل فوق یک اتصال استاندارد straight در کابل های CAT5 را نشان می دهد که از آن به منظور اتصال یک PC به هاب استفاده می گردد . ممکن است با مشاهده شکل فوق انتظار داشته باشید که +TX یک طرف به +TX طرف دیگر متصل گردد (عملا" این اتفاق نیافتاده است). زمانی که یک PC به هاب متصل می گردد، هاب به صورت اتوماتیک و با استفاده از مدارات داخلی خود کابل را X-over نموده و بدین ترتیب، پین شماره یک از کامپیوتر (+ TX) به پین شمار یک هاب (+ RX) متصل می گردد. در صورتی که هاب عملیات x-over را انجام ندهد (در زمان استفاده از پورت Uplink) ، پین شماره یک کامپیوتر (+ TX) به پین شماره یک هاب (+ TX) متصل می گردد . بنابراین مهم نیست که چه نوع عملیاتی را با پورت HUB انجام می دهیـــم (Uplink و یا نرمال)، سیگنال های نسبت داده شده به هشت پین سمت PC، همواره یکسان باقی مانده و هاب با توجه به نوع استفاده از پورت (نرمال و یا Uplink) عملیات لازم را انجام خواهد داد.

نحوه عملکرد خطوط T1

اکثر شما با یک خط مخابراتی معمولی آشنا هستید. در این نوع خطوط از یک زوج سیم مسی که مسئولیت انتقال صوت را به صورت سیگنال های آنالوگ برعهده دارد، استفاده می گردد. زمانی که این نوع خطوط را به یک مودم معمولی متصل می نمائیم، امکان انتقال داده تا ۳۰ کیلو بیت در ثانیه فراهم می گردد.

با توجه به تحولات گسترده در عرصه مخابراتی، اکثر شرکت های مخابراتی درصدد انتقال تمامی ترافیک صوتی خود به صورت دیجیتال در مقابل آنالوگ می باشند. در این رابطه می بایست خط آنالوگ شما به یک سیگنال دیجیتال تبدیل گردد. بدین منظور در هر ثانیه ۸۰۰۰ الگو و با دقت هشت بیت، نمونه برداری می گردد (٦٤،٠٠٠ بیت در ثانیه). در حال حاضر به منظور انتقال داده های دیجیتال عموما" از فیبرنوری استفاده می گردد. در این رابطه شرکت های مخابراتی از گزینه های متفاوتی در خصوص ظرفیت هر خط فیبر نوری، استفاده می نمایند. در صورتی که محل کار شما از یک خط T1 استفاده می نماید، نشاندهنده این موضوع است که شرکت مخابرات و سایر شرکت های عرضه کننده سرویس فوق، یک خط فیـــبرنوری را تا محل اداره شما آماده نموده اند. (یک خط T1 ممکن است به صورت مسی نیز ارائه گردد). یک خط T1 قادر به حمل ٢٤ کانال صوتی دیجیتال و یا انتقال داده با میزان ٥٤٤ / ١ مگابیت در هر ثانیه است.

در صورتی که خط T1 به منظور مبادلات تلفنی استفاده می گردد، خط فوق به سیستم تلفن اداره شما متصل می گردد. در صورتی که از خط T1 به منظور انتقال داده استفاده می گردد، خط فوق به روتر شبکه متصل می گردد.

یک خط T1 قادر به حمل حدود ١٩٢،٠٠٠ بایت در هر ثانیه است (٦٠ مرتبه بیش از یک مودم معمولی). ضریب اعتماد به اینگونه خطوط در مقایسه با یک مودم آنالوگ

بمراتب بیشتر است. یک خط T1 می تواند به صورت مشترک توسط کاربران متعددی استفاده شود (با توجه به نوع استفاده کاربران). مثلا" در صورت استفاده معمولی از اینترنت، صدها کاربر قادر به استفاده مشترک از یک خط T1 می باشند. در صورتی که تمامی کاربران فایل های MP3 را Download نموده و یا فایل های ویدئوئی را بطور همزمان مشاهده نمایند، ظرفیت و پهنای باند موجود جوابگو نخواهد بود، گرچه احتمال تحقق چنین شرایطی در یک مقطع زمانی خاص و بطور همزمان، کم می باشد.

یک شرکت بزرگ به چیزی بیش از یک خط T1 نیاز خواهد داشت. جدول زیر برخی از گزینه های متداول را نشان می دهد:

نوع خط	معادل
DS0	٦٤ کیلوبیت در هر ثانیه
ISDN	معادل دو خط DS0 به اضافه سیگنالینگ (١٦ کیلوبیت در هر ثانیه) و یا ١٢٨ کیلو بیت در ثانیه
T1	١ ٥٤٤ مگابیت در هر ثانیه (معادل ٢٤ خط DS0)
T3	٤٣ /٢٣٢ مگابیت در هر ثانیه (معادل ٢٨ خط T1)
OC3	١٥٥ مگابیت در هر ثانیه (معادل ٨٤ خط T1)
OC12	٦٢٢ مگابیت در هر ثانیه (معادل ٤ خط OC3)
OC48	٢ / ٥ گیگابیت در هر ثانیه (معادل ٤ خط OC12)
OC192	٩ / ٦ گیگابیت در هر ثانیه (معادل ٤ خط OC48)