عنوان:

شبکه های کامپیوتری

چکیده

شبکه های کامپیوتری امروزی فصل نویسی در انفورماتیک است . با وجود شبکه های کامپیوتری , محققین می توانند در اقصی نقاط دنیا تنها با فشردن کلیدهایی از صفحه کلید کامپیوتر , در چند ساعت بعد از تازه ترین اطلاعات موضوعات مورد نظر خود باخبر شوند .

تکنولوژی شبکه به سرعت در حال رشد است رشد و توسعه شبکه های کامپیوتری بر کسی پوشیده نیست مدت هاست که جمع آوری و پردازش اطلاعات توسط کامپیوتر انجام می شود .

علاوه بر این , کامپیوتر در توزیع اطلاعات و برقراری ارتباطات از طریق شبکه های کامپیوتری نقش مهمی را بازی می کند .

این پروژه تحقیقاتی که شبکه های کامپیوتری را مورد بررسی قرار می دهد که در ۴ فصل تقسیم بندی و ویرایش گردیده است .

فهرست :

مقدمه :

استفاده از شبکه های کامپیوتری در چندین سال اخیر رشد فراوانی کرده وسازمانها وموسسات اقدام به برپایی شبکه نموده اند . هر شبکه کامپیوتری باید با توجه به شرایط وسیاست های هر سازمان ، طراحی وپیاده سازی گردد. در واقع شبکه های کامپیوتری زیر ساخت های لازم را برای به اشتراک گذاشتن منابع در سازمان فراهم می آورند؛در صورتیکه این زیر ساختها به درستی طراحی نشوند، در زمان استفاده از شبکه مشکلات متفاوتی پیش آمده و باید هزینه های زیادی به منظور نگهداری شبکه وتطبیق آن با خواسته های مورد نظر صرف شود.

در زمان طراحی یک شبکه سوالات متعددی مطرح می شود:

-برای طراحی یک شبکه باید از کجا شروع کرد؟

-چه پارامترهایی را باید در نظر گرفت ؟

-هدف از برپاسازی شبکه چیست ؟

- انتظار کاربران از شبکه چیست ؟

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

-چه سرویس ها و خدماتی برروی شبکه ارائه خواهد شد؟

بطور کلی قبل از طراحی فیزیکی یک شبکه کامپیوتری ، ابتدا باید خواسته ها شناسایی وتحلیل شوند، مثلا در یک کتابخانه چرا قصد ایجاد یک شبکه را داریم واین شبکه باید چه سرویس ها وخدماتی را ارائه نماید؛ برای تامین سرویس ها وخدمات مورد نظر اکثریت کاربران ، چه اقداماتی باید انجام داد ؛ مسائلی چون

پروتکل مورد نظر برای استفاده از شبکه ، سرعت شبکه واز همه مهمتر مسائل امنیتی شبکه ، هریک از اینها باید به دقت مورد بررسی قرار گیرد. سعی شده است پس از ارائه تعاریف اولیه ، مطالبی پیرامون کاربردهای عملی آن نیز ارائه شود تا در تصمیم گیری بهتر یاری کند.

فصل اول

معرفی شبکه های کامپیوتری

معرفی شبکه های کامپیوتری

برای یک تکنسین شبکه دانستن اینکه کامپیوتر ها چطور با یکدیگر در یک شبکه کامپیوتری ارتباط برقرار می کنند بسیار مهم می باشد .

در این بخش اساس آنچه شبکه های کامپیوتری را میسازند،معرفی می گردد .در این جا نگاهی می اندازیم به توپولوژی های مختلف،سیستم عامل های شبکه و اطلاعات عمومی راجع به شبکه های کامپیوتری .جهت درک بهتر مطالب دیگر بخشها ،فهم اساسی م+طالب این بخش لازم می باشد.

این روزها استفاده از کامپیوترها در یک Settingخاص و حرفه ای بدون وجود شبکه تصور کردنی نیست. تکنسینهای شبکه باید تمامی ملزومات یک شبکه کامپیوتری را بدانند وبر نگهداری و اشکال زدایی

شبکه های خود مسلط باشند.

یک شبکه کامپوتری از دو جزء اساسی تشکیل شده : Entityکه اطلاعات و منابع را به اشتراک می گذارد،شبیه سرورها و ایستگاه های کاری . جزء دوم واسطه ایست که Entityها را قادر به ایجاد ارتباط با یکدیگر می سازد ، که کابل یا واسط بی سیم می باشد.

Entityها معمولا ایستگاه های کاری می باشند و واسط ها یک کابل یا یک واسط بی سیم مثل Infra red هستند.

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

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 .

۱-۱: تقسیم بندی بر اساس نوع وظایف :

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

Client Server:

در این نوع شبکه های کامپیوتری یعنی شبکه های مبتنی بر سرور، به تعداد محدودی از کامپیوتر ها وظیفه عمل به عنوان سرور داده می شود. در سازمان هایی که دارای بیش از ۱۰ کاربر در شبکه خود هستند، استفاده از شبکه های Peer to Peer نامناسب بوده و شبکه های مبتنی بر سرور ترجیح داده می شوند. در این شبکه ها از سرور اختصاصی برای پردازش حجم زیادی از درخواست های کامپیوترهای سرویس گیرنده استفاده می شود و آنها مسئول حفظ امنیت اطلاعات خواهند بود. در شبکه های مبتنی بر سرور، مدیر شبکه، مسئول مدیریت امنیت اطلاعات شبکه است و بر تعیین سطوح دسترسی به منابع شبکه مدیریت می کند. بدلیل اینکه اطلاعات در چنین شبکه هایی فقط روی کامپیوتر یا کامپیوتر های سرور متمرکز می باشند، تهیه نسخه های پشتیبان از آنها ساده تر بوده و تعیین برنامه زمانبندی مناسب برای ذخیره سازی و تهیه نسخه های پشتیبان از اطلاعات به سهولت انجام می پذیرد. در چنین شبکه هایی می توان اطلاعات را روی چند سرور نگهداری نمود، یعنی حتی در صورت از کار افتادن محل ذخیره اولیه اطلاعات (کامپیوتر سرور اولیه)، اطلاعات همچنان در شبکه موجود بوده و سیستم می تواند به صورت روی خط به کارکردخود ادامه دهد. به این نوع از سیستم ها Redundancy Systems یا سیستم های یدکی می گویند.

برای بهره گیری از مزایای هر دو نوع از شبکه ها، معمولاً سازمان ها از ترکیبی از شبکه های نظیر به نظیر و مبتنی بر سرور استفاده می کنند. این نوع از شبکه ها، شبکه های ترکیبی یا Combined Network نام دارند. در شبکه های ترکیبی دو نوع سیستم عامل برای تامین نیازهای شبکه مورد استفاده قرار می گیرند. به عنوان مثال یک سازمان می تواند از سیستم عامل Windows NT Server برای به اشتراک گذاشتن اطلاعات مهم و برنامه های کاربردی در شبکه خود استفاده کنند. در این شبکه، کامپیوتر های Client می توانند از سیستم عامل ویندوز ۹۵ استفاده کنند. در این وضعیت، کامپیوتر ها می توانند ضمن قابلیت دسترسی به اطلاعات سرور ویندوز NT، اطلاعات شخصی خود را نیز با دیگر کاربران به اشتراک بگذارند.

:Peer-To-Peer

در یک شبکه نظیر به نظیر یا Peer to Peer، بین گره های شبکه هیچ ترتیب یا سلسله مراتبی وجود ندارد و تمام کامپیوتر های واقع در شبکه از اهمیت یا اولویت یکسانی برخوردار هستند. به شبکه Peer to Peer یک گروه کاری یا Workgroup نیز گفته می شود. در این نوع از شبکه ها هیچ کامپیوتری در شبکه به طور اختصاصی وظیفه ارائه خدمات همانند سرور را ندارد. به این جهت هزینه های این نوع شبکه پایین بوده و نگهداری از آنها نسبتاً ساده می باشد. در این شبکه ها براساس آن که کدام کامپیوتر دارای اطلاعات مورد نیاز دیگر کامپیوتر هاست، همان دستگاه نقش سرور را برعهده می گیرد. و براساس تغییر این وضعیت در هر لحظه هر یک از کامپیوتر ها می توانند سرور باشند. و بقیه سرویس گیرنده. به دلیل کارکرد دوگانه هر یک از کامپیوتر ها به عنوان سرور و سرویس گیرنده، هر کامپیوتر در شبکه لازم است تا بر نوع کارکرد خود تصمیم گیری نماید. این فرایند تصمیم گیری، مدیریت ایستگاه کاری یا سرور نام دارد. شبکه هایی از نوع نظیر به نظیر مناسب استفاده در محیط هایی هستند که تعداد کاربران آن بیشتر از ۱۰ کاربر نباشد.

سیستم عامل هایی نظیر Windows ۹X، Windows NT Workstation یا Windows for Workgroup نمونه هایی از سیستم عامل های با قابلیت ایجاد شبکه های نظیر به نظیر هستند. در شبکه های نظیر به نظیر هر کاربری تعیین کننده آن است که در روی سیستم خود چه اطلاعاتی می تواند در شبکه به اشتراک گذاشته شود. این وضعیت همانند آن است که هر کارمندی مسئول حفظ و نگهداری اسناد خود می باشد.

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

۲-۱: 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 .

توپولوژی های مختلفی شبکه های کامپیوتری را می سازند.

Bus Star Mesh Ring Wireless

توپولوژی Bus :

یکی از رایجترین توپولوژی ها برای پیاده سازی شبکه های LAN است . در مدل فوق از یک کابل بعنوان ستون فقرات اصلی در شبکه استفاده شده و تمام کامپیوترهای موجود در شبکه (سرویس دهنده ، سرویس گیرنده) به آن متصل می گردند. این کار از لحاظ منطقی ممکن است عجیب باشد ، اما تنظیم و نصب چنین شبکه ای بسیار ساده می با شد.در توپولوژی Busبیشر از کابل کواکسیال استفاده می شود.

در توپولوژی Busدر آن واحد تنها یک کامپیوتر می تواند یک Packetرا انتقال دهد.در این توپولوژی کامپیوتر ها تنها Packetهایی را که شامل آدرس آنهاست می پذیرند.یک Packetازلحظه ارسال شدن توسط کامپیوتر مبداء تا لحظه دریافت توسط کامپیوتر مقصد در طول مسیر در حرکت است . این بدان معنی است که شبکه تا زمانی که کامپیوتر مقصد آن Packetرا بپذیرد اشغال می شود.در توپولوژی Bus برای جلوگیری از bounce،اجزایی به نام ترمیناتور را در دو سر انتهایی کابل قرار می دهند .یک ترمیناتور سیگنالهای الکتریکی را جذب کرده و کابل را آزاد می کند ، بنابراین کامپیوترها می توانند Packetها را به شبکه بفرستند .

توپولوژی Busیک توپولوژی بی بهره است . این بدان معنی است که در توپولوژی Busیک کامپیوتر اطلاعات را دریافت میکند ومی فرستد و هیچ data یی را دوباره تولید نمی کند ،بنابر این اگر یک کامپیوتر در یک شبکه failشود شبکه از کار خواهد افتاد .

یکی از مزایای توپولوژی Busهزینه آن می باشد.توپولوژی Busکمتر از Starویا Meshکابل مصرف می کند.دیگر مزیت آن سادگی نصب این نوع توپولوژی می باشد .

مهمترین عیب توپولوژی Busمشکل بودن عیب یابی آن می باشد.

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

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

نصب کابل در یک شبکه Bus:

۱- همه کامپیوتر ها در کارت شبکه یک اتصال دهنده BNCدارند.

۲- کابل را بین کامپیوتر ها روی یک خط رد کنید ، طول کابل بیش از ۱۸۵ متر نباشد.

۳- از یک ابزار Crimpingبرای جاگذاری اتصال دهنده BNCدر انتهای تمام کابل ها استفاده کنید .

۴- یک T-connectorروی همه رابطهای BNCقرار دهید .

۵- انتهای هر کابل را به T-connectorمتصل کنید .

۶- ترمیناتور را روی دو کامپیوتری که در انتهای Busقرار دارند و هر کدام یک سوکت T-connector خالی نیز دارند وصل کنید.

توپولوژی Star:

در این نوع توپولوژی همانگونه که از نام آن مشخص است ، از مدلی شبیه "ستاره" استفاده می گردد.در این توپولوژی همه کامپیوتر ها به واسطه یک هاب یا سوییچ به هم متصل می شوند.

یکی از مزایای توپولوژی ستاره ای تمرکز در کابل کشی است.در یک هاب اگر کابلی قطع شود بر دیگر ایستگاه های کاری تاثیری ندارد.تمرکز در اجزای شبکه ،قدرت مدیریت را بالا می برد.مدیریت متمرکز و مانیتورینگ ترافیک شبکه برای موفقیت شبکه می تواند اساسی و حیاتی باشد. با یک پیکربندی ستاره ای امکان اضافه کردن ویا تغیی در پیکربندی آسان می باشد زیرا همه اتصالات در یک نقطه متمرکز هستند .

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 یک دستگاه . نقاط اتصالی در شبکه ذاتا" مستعد اشکال هستند. در توپولوژی STAR اشکال در یک اتصال ، باعث خروج آن خط از شبکه و سرویس و اشکال زدائی خط مزبور است . عملیات فوق تاثیری در عملکرد سایر کامپیوترهای موجود در شبکه نخواهد گذاشت .

- کنترل مرکزی و عیب یابی . با توجه به این مسئله که نقطه مرکزی مستقیما" به هر ایستگاه موجود در شبکه متصل است ، اشکالات و ایرادات در شبکه بسادگی تشخیص و مهار خواهند گردید.

- روش های ساده دستیابی . هر اتصال در شبکه شامل یک نقطه مرکزی و یک گره جانبی است . در چنین حالتی دستیابی به محیط انتقال جهت ارسال و دریافت اطلاعات دارای الگوریتمی ساده خواهد بود.

معایب توپولوژی STAR :

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

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

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

توپولوژی Mesh:

این نوع توپولوژی در شبکه بندی زیاد رایج نمی باشد.در توپولوژی Meshهر کامپیوتر با دیگر کامپیوترهای شبکه یک اتصال دارد.

بزرگترین مزیت توپولوژی Mesh، Fault toleranceمی باشد. این بدان معنی است که اگر یک شکست یا پارگی در کابل بوجود بیاید ،جریان داده می تواند دوباره مسیردهی شود.

عیب این توپولوژیِ آن است که بکارگیری و مدیریت شبکه Meshبه دلیل اتصالات متعدد وزیاد بسیار مشکل است .هزینه نیزدر این نوع توپولوژی زیاد می باشد .

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.

توپولوژی Ringمداریست که نقطه شروع وپایان ندارد.در این توپولوژی به ترمیناتور نیازی نیست .سیگنالها یک مسیر دایره ای را تا زمانی که یک کامپیوتر آنها را به کامپیوتر دیگر رد می کند ،طی میکنند.هر کامپیوتر آدرس مقصد Packetرا چک می کند و آن را مثل یک تکرار کننده عبور می دهد.

اگر یکی از کامپیوترهای شبکه حلقوی دچار اشکال شود،تمامی شبکه از کار میفتد.

مزایای توپولوژی Ring:

بهترین قابلیت این توپولوژی این است که همه کامپیوترها امکان دسترسی و ارتباط مساوی بر روی شبکه دارند .(در توپولوژی Busو Starفقط یک ایستگاه کاری در آن واحد با شکه ارتباط دارد.)در توپولوژی حلقوی کامپیوتر هایی که حجم زیادی از اطلاعات را روی شبکه می فرستند از ارتباط دیگر

کامپیوتر ها جلوگیری نمی کنند .دیگر مزایای Ringعبارتند از:

-*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 بمنظور کابل کشی ضرورتی نخواهد داشت .

- مناسب جهت فیبر نوری . استفاده از فیبر نوری باعث بالا رفتن نرخ سرعت انتقال اطلاعات در شبکه است. چون در توپولوژی فوق ترافیک داده ها در یک جهت است ، می توان از فیبر نوری بمنظور محیط انتقال استفاده کرد.در صورت تمایل می توان در هر بخش ازشبکه از یک نوع کابل بعنوان محیط انتقال استفاده کرد . مثلا" در محیط های ادرای از مدل های مسی و در محیط کارخانه از فیبر نوری استفاده کرد.

معایب شبکه با توپولوژی Ring:

بزرگترین مشکل در توپولوژی Ringاین است که اگر یک کامپیوتر از کار بیفتد ، دچار خطا شود ویا کابل قطع شود کل شبکه از کار میفتد.

مفهوم توپولوژی Ringاین است که حلقه شکسته نمی شود و سیگنالها از یک ایستگاه به ایستگاه دیگر پرش می کنند .

عیب دیگر توپولوژی حلقوی آن است که اگر تغییراتی در کابل یا شبکه ویا ایستگا های کاری اعمال کنیم مانند جابجایی و یا قطع موقت اتصالات ،شبکه را دچار اختلال و وقفه می کند .بنابر این مشکلات این نوع توپولوژی را می توان به صورت زیر بیان کرد :

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

- اشکال زدائی مشکل است . بروز اشکال در یک گره می تواند روی تمام گرههای دیگر تاثیر گذار باشد. بمنظور عیب یابی می بایست چندین گره بررسی تا گره مورد نظر پیدا گردد.

- تغییر در ساختار شبکه مشکل است . در زمان گسترش و یا اصلاح حوزه جغرافیائی تحت پوشش شبکه ، بدلیل ماهیت حلقوی شبکه مسائلی بوجود خواهد آمد .

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

توپولوژی Wireless:

یک توپولوژی بی سیم آن است که در آن کمترین کابل برای اتصالات سیم ها بکار رفته است.در این توپولوژی شبکه از یک فرستنده استفاده می کند که Packetها را با بکارگیری فرکانسهای رادیویی منتشر می کند.شبکه دارای فرستنده های مخصوصی است که Cellنامیده می شوند.کامپیوترهاو اجزای شبکه یک فرستنده/گیرنده مخصوص دارند که آنها را برای دریافت انتشارات و انتقال داده ها ی درخواست شده به Cell،هدایت می کند.

حالت دیگر شبکه بی سیم نوعی است که از آنتن رادیویی در نزدیکی ساختمان استفاده می کند.این آنتن یک Cellرا برای احاطه محیط اطراف هدایت می کند.در یک ترکیب Campus-Typeاین دسترسی بهترین راه است .

شبکه بی سیم می تواند با ارتباطات Infraredسازگار باشد،مشابه کنترل تلوزیون اما این نوع ارتباط آهسته و کند است و یک خط مستقیم برای ایجاد ارتباط برای کار نیاز دارد.

این نوع شبکه بیشتر برای Laptop یا Laptopوپرینتر مفید است.

بهترین مزیت این شبکه ها نداشتن کابل کشی است .شبکه بی سیم به یک Backbonاساسی برای آنچه می خواهد به Cellهای بی سیم متصل شود ،احتیاج دارد .

Backbonبخشی از کابل اصلی است که کابل های کوچکتر به آن متصل می شوند .

۳-۱: 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 صورتیکه 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 و گران)

- BlueTooth
- IrDA
- (SWAP)(HomeRF)
- (Wi-Fi)(WECA)

شبکه های Bluetooth در حال حاضر عمومیت نداشته و بنظر قادر به پاسخگوئی به کاربران برای شبکه ها ی با سرعت بالا نمی باشند.(Infrared Data Association(IrDA استانداردی بمنظور 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 تبین 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 ۸۰۲.۱۱ توسط موسسه IEEE عرضه گردید. در استاندارد فوق دو روش بمنظور ارتباط بین دستگاهها با سرعت دو مگابیت در ثانیه مطرح شد. دو روش فوق بشرح زیر می باشند :

- Direct-sequence spread spectrum DSSS
- (Frequency-hopping spread spectrum)(FHSS)

دو روش فوق از تکنولوژی(Frequency-shift keying(FSK استفاده می نمایند. همچنین دو روش فوق از امواج رادیوئی Spread-spectrum در محدوده ۴/ ۲ 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" ۴۰۰ میلی ثانیه) ، بنابراین می توان از چندین شبکه FHSS 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 Shared Wireless Access(SWAP 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 بمنظور 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 PCI , ISA و یا PCMCIA ایجاد(ساخته) می گردد. در صورتیکه 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 بعنوان یک منبع اشتراکی مورد استفاده قرار گیرند.

اکثر شبکه های SWAP بصورت " نظیر به نظیر " می باشند . برخی از تولیدکنندگان اخیرا" بمنظور 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 :

Compatibility Alliance Wireless Ethernet(WECA)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 b۸۰۲.۱۱ ، هر دستگاه قادر به برقراری ارتباط با سرعت یازده مگابیت در ثانیه است . در صورتیکه 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 فضای باز و ۲۵۰ تا ۴۰۰ فوت / ۷۶ تا ۱۲۲ متر در فضای بسته)
- با شبکه های کابلی بسادگی ترکیب می گردد.
- با دستگاههای DSSS ۸۰۲.۱۱ (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 بمنظور 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 بمنظور 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.

۴-۱: سیستم عامل شبکه:

حالا که یک تصور کلی از طرح یا همبندی شبکه ها داریم بهتر است به سیستم عامل شبکه (NOS) نگاهی بیندازیم .تمرکز ما بر روی سه سیستم عاملی است که در شبکه زیاد به کار میروند.

Microsoft Windows NT/Windows ۲۰۰۰

Network Novell

Unix

سیستم عامل شبکه در دو روش می تواند عمل کند .در یک محیط نظیر به نظیر هر ایستگاه کاری روی یک شبکه بصورت مساوی برای مدیریت منابع مسئول است .هر ایستگاه کاری منفرد می تواند منابعش را با دیگر سیستم های شبکه به اشتراک بگذارد.

در محیط Client/Serverبه یک دسترسی متمرکز برای NOSاحتیاج است.اگر به عنوان مدیر شبکه یک ماشین را به عنوان Serverتعریف کنید ،می توانید اشتراک منابع شبکه را متمرکز کنید .

مثال هایی از سیستم عامل های Server،ویندوز NTو ۲۰۰۰سرور می باشند.Clientهای ممکن برای این سیستم عامل ها ویندوز xpحرفه ای و ۲۰۰۰حرفه ای ، Windows NT workstation، Win

ME، Win ۹۸ ، Win ۹۵ ، Win ۳.۱و

MS Dosمی باشند.

۵-۱: کلاینت ها و منابع :

جزء اصلی موفقیت شبکه با یک NOSنرم افزار clientاست.در هر دو محیط نظیر به نظیر و client/serverشما به نرم افزار clientنیاز دارید.یک دلیل موفقیت NTو WIN۲۰۰۰این است که این دو clientهای مختلفی را حمایت می کنند.

در یک محیط متمرکز یک کامپیوتر باید رئیس شبکه باشد ،کامپیوتری که به همه کامپیوترهای دیگر سرویس می دهد Serverنام دارد.کلمه Serverاز این واقعیت می آید که کامپیوتر Serverاحتیاجات کامپیوترهای دیگر را در یک شبکه متمرکز سرویس می دهد. Windows NT Serverو Windows Server ۲۰۰۰طراحی شده اند برای اینکه یک ماشین قدرتمند باشند جهت سرویس دهی دیگر کامپیوترها.به همین ترتیب Windows NT Workstation و Windows ۲۰۰۰ Profetionalجهت اجرا روی یک دستگاه client طراحی شده اند.

نرم افزاری که برای دستگاه سرویس دهنده طراحی شده ،به سادگی منابع روی شبکه را مدیریت و کنترل می کند.نرم افزار Serverحقیقتا برای استفاده مدیر شبکه طراحی شده است .مدیر شبکه با بکار گیری این نرم افزار می تواند اعمالی از قبیل کنترل شبکه ، مسیردهی ، کنترل خطا ومدیریت کاربر را انجام دهد .

سرویس های دایرکتوری :

در ویندوز NTسرور اصلی که Acountمحرمانه را نگهداری می کند Domail Controllerنامیده می شود. Domain Controllerدسترسی کاربران به شبکه را کنترل و مدیریت می کند.وقتی کاربری به یک ایستگاه کاری در شبکه وارد می شود کلمه عبور او توسط یک Domail Controllerبررسی و

تصدیق می شود.

۶-۱: پروتکل :

فرآیند به اشتراک گذاشتن اطلاعات نیازمند ارتباط همزمان شده ای بین کامپیوتر های شبکه است. برای ایجاد سهولت در این فرایند، برای هر یک از فعالیت های ارتباط شبکه ای، مجموعه ای از دستور العمل ها تعریف شده است. هر دستور العمل ارتباطی یک پروتکل یا قرارداد نام دارد. یک پروتکل تامین کننده توصیه هایی برای برقراری ارتباط بین اجزای نرم افزاری و سخت افزاری در انجام یک فعالیت شبکه ای است. هر فعالیت شبکه ای به چندین مرحله سیستماتیک تفکیک می شود. هر مرحله با استفاده از یک پروتکل منحصر به فرد، یک عمل مشخص را انجام می دهد. این مراحل باید با ترتیب یکسان در تمام کامپیوترهای واقع در شبکه انجام شوند. در کامپیوتر مبدا مراحل ارسال داده از لایه بالایی شروع شده و به طرف لایه زیرین ادامه می یابد. در کامپیوتر مقصد مراحل مشابه در جهت معکوس از پایین به بالا انجام می شود. در کامپیوتر مبدا، پروتکل اطلاعات را به قطعات کوچک شکسته، به آن ها آدرس هایی نسبت می دهند و قطعات حاصله یا بسته ها را برای ارسال از طریق کابل آماده می کنند. در کامپیوتر مقصد، پروتکل ها داده ها را از بسته ها خارج کرده و به کمک نشانی های آن ها بخش های مختلف اطلاعات را با ترتیب صحیح به هم پیوند می دهند تا اطلاعات به صورت اولیه بازیابی شوند.

پروتکل های مسئول فرآیندهای ارتباطی مختلف برای جلوگیری از تداخل و یا عملیات ناتمام، لازم است که به صورت گروهی به کار گرفته شوند. این عمل به کمک گروهبندی پروتکل های مختلف در یک معماری لایه ای به نام Protocol Stack یا پشته پروتکل انجام می گیرد. لایه های پروتکل های گروه بندی شده با لایه های مدل OSI انطباق دارند. هر لایه در مدل OSI پروتکل مشخصی را برای انجام فعالیت های خود بکار می برد. لایه های زیرین در پشته پروتکل ها تعیین کننده راهنمایی برای اتصال اجزای شبکه از تولیدکنندگان مختلف به یکدیگر است.

لایه های بالایی در پشته پروتکل ها تعیین کننده مشخصه های جلسات ارتباطی برای برنامه های کاربردی

می باشند. پروتکل ها براساس آن که به کدام لایه از مدل OSI متعلق باشند، سه نوع طبقه بندی می شوند. پروتکل های مربوط به سه لایه بالایی مدل OSI به پروتکل های Application یا کاربرد معروف هستند. پروتکل های لایه Application تامیین کننده سرویس های شبکه در ارتباط بین برنامه های کاربردی با یکدیگر هستند. این سرویس ها شامل انتقال فایل، چاپ، ارسال پیام و سرویس های بانک اطلاعاتی هستند. پروتکل های لایه نمایش یا Presentation وظیفه قالب بندی و نمایش اطلاعات را قبل از ارسال بر عهده دارند. پروتکل های لایه جلسه یا Session اطلاعات مربوط به جریان ترافیک را به داده ها اضافه می کنند.

پروتکل های نوع دوم که به پروتکل های انتقال (Transparent) معروف هستند، منطبق بر لایه انتقال مدل OSI هستند. این پروتکل ها اطلاعات مربوط به ارسال بدون خطا یا در واقع تصحیح خطا را به داده ها می افزایند. وظایف سه لایه زیرین مدل OSI بر عهده پروتکل های شبکه است. پروتکل های لایه شبکه تامیین کننده فرآیندهای آدرس دهی و مسیریابی اطلاعات هستند. پروتکل های لایه Data Link اطلاعات مربوط به بررسی و کشف خطا را به داده ها اضافه می کنند و به درخواست های ارسال مجدد اطلاعات پاسخ می گویند. پروتکل های لایه فیزیکی تعیین کننده استاندارد های ارتباطی در محیط مشخصی هستند.

۷-۱: عملکرد لایه های مختلف:

هر لا یه عملکرد مخصوصی دارد که آن را تعریف می کند.برخی عملیات مثل کنترل خطا و کنترل جریان ،در بیش از یک لایه تعریف شده اند.این بدان معنی نیست که این عملیات مجبورند در دو لایه اجرا شوند.فراموش نکنید که OSI یک مدل است .یک طراح ممکن است کنترل خطا را در یک لایه ، ودیگر طراح آن را در لایه ای دیگر استفاده کند.اینها هما مربوط به اهداف طراح می باشد.

لایه فیزیکی:

لایه زیرین ساختار OSI مربوط است به انتقال بیتهایی از داده به واسط شبکه. لایه فیزیکی واسط را

مشخص نمی کند بلکه دسترسی به آن را معین می کند.این شامل توپولوژی فیزیکی شبکه یا ساختار شبکه،جنبه های الکتریکی ،فیزیکی واسط های بکار رفته،وEncoding و زمانبندی انتقال و دریافت بیت می باشد.این لایه مربوط به تکرار کننده است .تکرارکننده سیگنالهای الکتریکی را تقویت می کند.

پیوند داده:

این لایه جریانات مربوط به انتقالات روی شبکه را کنترل می کند.(لایه شبکه که در قسمت بعد مطرح شده ،عملیات ضروری را برای انتقال به آنطرف یک شبکه فیزیکی انجام می دهد.)وقتی پیغامی از شبکه دریافت می شود این لایه اطلاعات را دوباره در فریم هایی جهت فرستادن به لایه های بالایی ، جمع آوری می کند .

مدل ۸۰۲ لایه پیوند داده را به دو زیر لایه تقسیم می کند ،کنترل پیوند منطقی (LLC) و کنترل دسترسی Media(MAC).

لایه LLCارتباط بین دو وسیله را آغاز و حفظ می کند.زمانیکه ما دادهای را از ایستگاه کاری خود به سمت سرور می فرستیم ،زیر لایه LLCاست که یک اتصال با سرور برقرار میسازد.

زیر لایهMAC چند وسیله را قادر می سازد تا Media را به اشتراک بگذارند.بیشتر LAnها بیش از دو کامپیوتر دارند و زیر لایه MAC تعیین کننده این است که کدام کامپیوتر اجازه استفاده از شبکه را دارد.

مهمترین کار دیگر لایه پیوند داده آدرس دهی فیزیکی وسایل شبکه است.MAc ،آدرس فیزیکی وسایل شبکه را مشخص می کند.(معمولا MAC Address نامیده می شود).هر وسیله روی شبکه باید یک MAC Address منحصر بفرد داشته باشد والا شبکه نخواهد فهمید که اطلاعات زمان درخواست یک شخص به کجا باید فرستاده شوند .

در پایان لایه پیوند داده کنترل جریان و تصحیح خطا بین وسایل در یک شبکه مشابه را مدیریت می کند .

لایه شبکه :

لایه شبکه یکی از مهمترین و پیچیده ترین لایه هاست.این لایه آدرس دهی و رساندن Packetها روی یک شبکه پیچیده را کنترل و مدیریت می کند.شبکه های داخلی با وسایلی به نام روتر متصل شده اند.روتر دستگاهی است که جداول مسیردهی و الگوریتمهای مسیردهی را برای چگونگی فرستادن داده ها از یک شبکه به دیگر شبکه ها ،مورد استفاده قرار میدهد.

هر شبکه باید یک آدرس داشته باشد که این آدرس آن را از شبکه های دیگر مجزا سازد.وقتی داده ای را از یک شبکه به شبکه دیگر می فرستیم روتر ها در طول راه ،آدرس شبکه را برای تعیین گام بعدی در مسیر استفاده می کنند.

لایه انتقال:

وظیفه این لایه حفظ و اطمینان از رسیدن صحیح داده به مقصدش می باشد .لایه انتقال بسیار دقیق وسخت کار می کند .این لایه متاثر از لایه شبکه است .

لایه Session:

این لایه دیالوگ بین کامپیوتر ها را مدیریت می کند .لایه Session سه نوع دیالوگ را بکار می برد:

Simplex، Half Duplex و Fuul Duplex .

Simplex:

اطلاعات را تنها در یک مسیر جاری می سازد.از آنجا که دیالوگ یکطرفه است اطلاعات تنها می توانند فرستاده فرساتده شوند .یک مثال از دیالوگ یکطرفه اخطار عمومی (PA)در یک ساختمان بزرگ می باشد.اخطار داده می شود اما سیستم PA قادر نیست از شنونده پاسخی دریافت کند.

Half Duplex:

به داده ها امکان می دهد که در دو مسیر جریان داشته باشند ولی در آن فقط یک مسیر باز است.بی سیم یک مثال واضح از این نوع دیالوگ می باشد.

Full Duplex:

این متد امکان جریان یافتن در دو مسیر به طور همزمان را به داده ها می دهد .این نوع دیالوگ انعطاف پذیر تر است اما به متد های ترکیبی بیشتری نیاز دارد.تلفن اصلی ترین مثال ارتباط Full Duplex می باشد.

زمانی که یک Session تشکیل میگردد مراحل زیر را شامل می شود :در ابتدا در خواست کننده ارتباط، سرویس را آغاز می کند و قوانینی برای ایجاد ارتباط ایجاد می شود.به محض اینکه قاعده ها ایجاد شدند مرحله انتقال داده شروع می شود.هر دو طرف می دانند که چگونه باید با یکدیگر صحبت کنند.در پایان جلسه کامل شده و ارتباط پایان می یابد.

لایه نمایش:

لایه نمایش بررسی می کند که داده های فرستاده شده از لایه تقاضا و دریافت شده توسط لایه جلسه در فرمت مناسب هستند یا خیر.

انواع مختلف کامپیوتر میتوانند داده های یکسان را به صورتهای مختلف ترجمه کنند.استاندارد شبکه فرمت مناسبی را برای داده های انتقالی تعریف می کند.زمانی که لایه نمایش داده ها را از لایه Application دریافت کرد قبل از فرستادن آنها به شبکه از درستی فرمت آنها مطمئن می شود.اگر داده ها در فرمت مناسب نبودند آنها را بر می گرداند.لایه نمایش دربرابر داده های دریافتی از لایه Session نیز همین عملیات را انجام می دهد.

لایه Application:

این لایه یک واسط بیطرف استوار برای شبکه است.لایه Application شامل راه های فراوانی است برا ی درخواست ذخیره فایلها در یک فایل سرور شبکه یا چاپ با یک چاپگر شبکه و ...این لایه منابع قابل دسترسی یک سیستم را به بقیه شبکه معرفی می کند.

مثال:

ما درقسمتهای قبل مطالبی درباره مدل OSI خواندیم،حال می توانیم این مطالب را در مثال زیر به کار بریم.

فرض کنیم می خواهیم فایلی را از سرویس دهنده FTP(FTP Server)، Download کنیم.

پروسه ای که برای انتقال فایل بین کامپیوترها روی سیستم ما اتفاق میفتد به شرح زیر است:

۱ - رابط FTPباز شده و PC راه دور ازاین رابط انتخاب می شود تا ارتباط با آن برقرار شود.

۲ - رابط FTP روی لایه Application اجرا می شودو اطلاعات را به لایه نمایش می دهد.این لایه تقاضا را برای فهم دیگر کامپیوترها، به فرم اصلی برمیگرداند .

۳ - درخواست به لایه Session فرستاده می شود واتصال برقرار می شود.

۴ - packetهای داده به لایه انتقال فرستاده می شوند.اگر برای انتقال روی واسط شبکه نیاز باشد، این لایه دوباره آنها را تقسیمبندی می کند .

۵ - packetهای داده به لایه شبکه فرستاده می شوند.

۶ - توقف بعدی در لایه پیوند داده هاست که آدرس فیزیکی مقصد packetها در این لایه تکمیل می شود.

۷ - در پایان packetهای داده به لایه فیزیکی فرستاده می شوند جاییکه به سیگنالهای الکتریکی تبدیل شده و به واسط شبکه انتقال داده می شوند. واسط شبکه می تواند یک خط تلفن باشد .

۸ - packetهای داده به سرویس دهنده FTP هدایت می شوند و فیل درخواستی شما برگردانده می

شود(در مسیری مشابه گامهای ۱ تا ۷).

۸-۱: معرفی برخی اصطلاحات شبکه های کامپیوتری :

Server :

یکی از مهمترین اجزای شبکه های کامپیوتری، کامپیوتر سرور است. سرور مسئول ارائه خدماتی از قبیل انتقال فایل، سرویس های چاپ و غیره است. با افزایش حجم ترافیک شبکه، ممکن است برای سرور مشکلاتی بروز کند. در شبکه های بزرگ برای حل این مشکل، از افزایش تعداد کامپیوترهای سرور استفاده می شود که به این سرور ها، سرور های اختصاصی گفته می شود. دو نوع متداول این سرور ها عبارتند از File and Print server و Application server. نوع اول یعنی سرویس دهنده فایل و چاپ مسئول ارائه خدماتی از قبیل ذخیره سازی فایل، حذف فایل و تغییر نام فایل است که این درخواست ها را از کامپیوتر های سرویس گیرنده دریافت می کند. این سرور همچنین مسئول مدیریت امور چاپگر نیز هست.

هنگامی که یک کاربر درخواست دسترسی به فایلی واقع در سرور را ارسال می کند، کامپیوتر سرور نسخه ای از فایل کامل را برای آن کاربر ارسال می کند. بدین ترتیب کاربر می تواند به صورت محلی، یعنی روی کامپیوتر خود این فایل را ویرایش کند.

کامپیوتر سرویس دهنده چاپ، مسئول دریافت درخواست های کاربران برای چاپ اسناد است. این سرور این درخواست ها را در یک صف قرار می دهد و به نوبت آن ها را به چاپگر ارسال می کند. این فرآیند Spooling نام دارد. به کمک Spooling کاربران می توانند بدون نیاز به انتظار برای اجرای فرمان Print به فعالیت برروی کامپیوتر خود ادامه دهند.

نوع دیگر سرور، Application Server نام دارد. این سرور مسئول اجرای برنامه های Client/Server و تامین داده های سرویس گیرنده است. سرویس دهنده ها، حجم زیادی از اطلاعات را در خود نگهداری می کنند. برای امکان بازیابی سریع و ساده اطلاعات، این داده ها در یک ساختار مشخص ذخیره می شوند. هنگامی که کاربری درخواستی را به چنین سرویس دهنده ای ارسال می کند. سرور نتیجه درخواست را به کامپیوتر کاربر انتقال می دهد. به عنوان مثال یک شرکت بازاریابی را در نظر بگیرید. این شرکت در نظر دارد تا برای مجموعه ای از محصولات جدید خود تبلیغ کند. این شرکت می تواند برای کاهش حجم ترافیک، برای مشتریان با طیف درآمدهای مشخص، فقط گروهی از محصولات را تبلیغ نماید.

علاوه بر سرور های یاد شده، در یک شبکه می توان برای خدماتی از قبیل پست الکترونیک، فکس، سرویس های دایرکتوری و غیره نیز سرورهایی اختصاص داد. اما بین سرور های فایل و Application Server ها تفاوت های مهمی نهفته است. یک سرور فایل در پاسخ به درخواست کاربر برای دسترسی به یک فایل، یک نسخه کامل از فایل را برای او ارسال می کند درحالی که یک Application Server فقط نتایج درخواست کاربر را برای وی ارسال می نماید.

MANs , WANs , LANs:

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 بمنظور ارسال اطلاعات
- نرخ پایین خطاء در ارسال اطلاعات با توجه به محدود بودن فاصله

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

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

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

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

فصل دوم

سخت افزار شبکه

۲-۱ : Cabling:

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

LANها با بکار گیری یکی از انواع کابل می توانند به هم متصل شوند.هر نوع کابل مزایا و معایب مخصوص به خود را دارد که در اینجا به برخی از آنها اشاره می کنیم.

سه نوع اصلی کابل عبارتند از : کابل کواکسیال، کابل زوج به هم تابیده و فیبر نوری.

۲-۱-۲ : Coaxial Cable:

یکی از مهمترین محیط های انتقال در مخابرات کابل کواکسیال و یا هم محور می باشد . این نوع کابل ها از سال ۱۹۳۶ برای انتقال اخبار و اطلاعات در دنیار به کار گرفته شده اند. در این نوع کابل ها، دو سیم تشکیل دهنده یک زوج ، از حالت متقارن خارج 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.

شکل ۱-۲

مزایای کابل های کواکسیال :

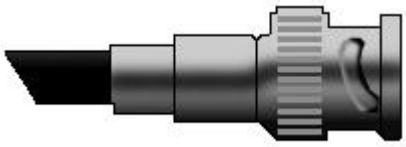
- قابلیت اعتماد بالا
- ظرفیت بالای انتقال ، حداکثر پهنای باند ۳۰۰ مگاهرتز
- دوام و پایداری خوب
- پایطن بودن مخارج نگهداری
- قابل استفاده در سیستم های آنالوگ و دیجیتال
- هزینه پائین در زمان توسعه
- پهنای باند نسبتا" وسیع که مورد استفاده اکثر سرویس های مخابراتی از جمله تله کنفرانس صوتی و تصویری است .

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

BNC :

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



شکل ۲-۲

۲-۱-۳ : فیبر نوری:

یکی از جدیدترین محیط های انتقال در شبکه های کامپیوتری ، فیبر نوری است . فیبر نوری از یک میله استوانه ای که هسته نامیده می شود و جنس آن از سیلیکات است تشکیل می گردد. شعاع استوانه بین دو تا سه میکرون است . روی هسته ، استوانه دیگری (از همان جنس هسته) که غلاف نامیده می شود ، استقرار می یابد. ضریب شکست هسته را با M۱ و ضریب شکست غلاف را با M۲ نشان داده و همواره M۲<M۱ است . در این نوع فیبرها ، نور در اثر انعکاسات کلی در فصل مشترک هسته و غلاف ، انتشار پیدا خواهد کرد. منابع نوری در این نوع کابل ها ، دیود لیزری و یا دیودهای ساطع کننده نور می باشند.منابع فوق ، سیگنال های الکتریکی را به نور تبدیل می نمایند.

شکل ۲-۳

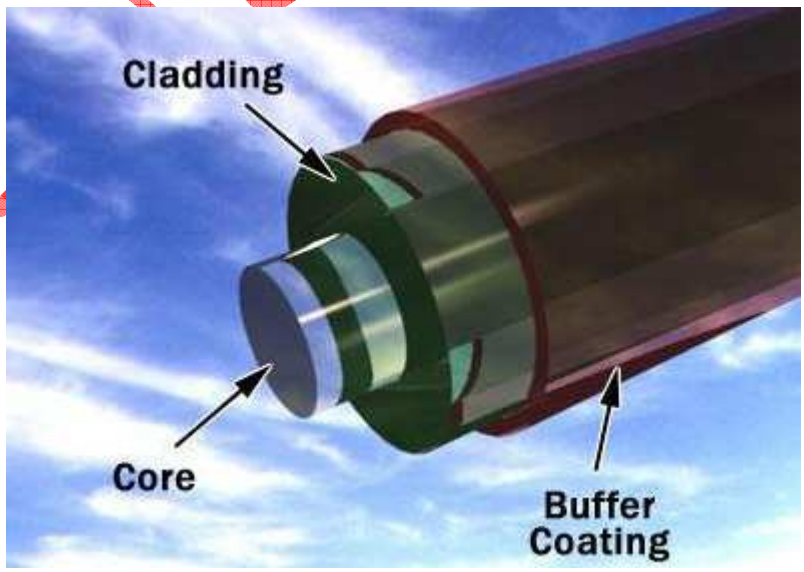
امروزه از فیبر نوری در موارد متفاوتی نظیر: شبکه های تلفن شهری و بین شهری ، شبکه های کامپیوتری و اینترنت استفاده بعمل می آید. فیبرنوری رشته ای از تارهای شیشه ای بوده که هر یک از تارها دارای

ضخامتی معادل تار موی انسان را داشته و از آنان برای انتقال اطلاعات در مسافت های طولانی استفاده می شود.

شکل ۴-۲

۴-۱-۲: 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.



شکل ۵-۲

یک فیبر نوری از سه بخش متفاوت تشکیل شده است :

- هسته (Core) . هسته نازک شیشه ای در مرکز فیبر که سیگنا ل 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 (Buffer Coating) . 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.

۵-۱-۲ : 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 مسفقیم 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. (مثلا" موج با طول ۸۵۰ نانومتر بین ۶۰ تا ۷۵ درصد در هر کیلومتر ، موج با طول ۱۳۰۰ نانومتر بین ۵۰ تا ۶۰ درصد در هر کیلومتر ، موج با طول ۱۵۵۰ نانومتر بیش از ۵۰ درصد در هر کیلومتر)

۶-۱-۲ : 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 جهانی 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 کاملا" بحرانی و توفانی را دارند. یکی 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 بسار زیاد (هزاران مایل) بوده و بمنظور برقرای ارتباط بین آنها از یک سیتستم مخابراتی مبتنی بر فیبر نوری استفاده گردد.

سیتستم 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 .

۲-۱-۷ :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 بیشتر است . متداولترین طول موج سیگنا ل های نوری ، ۸۵۰ نانومتر ، ۱۳۰۰ نانومتر و ۱۵۵۰ نانومتر است .

۸-۱-۲ : 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)

۹-۱-۲ :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 نور ی 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.

دو حادثه الکتریکی می تواند شبکه را قطع کند : cross-talk و نویزهای الکتریکی خارجی.

Cross-talk توسط فیلدهای الکتریکی در وایرهای مجاور که شامل سیگنالهای false هستند، تولید می

شود. نویزهای الکتریکی از لامپها ، موتورها و سیستم های رادیویی و منابع دیگر می آید .فیبر نوری در مقابل این نویز ها و تداخلات ایمن است .

معایب فیبر نوری :

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

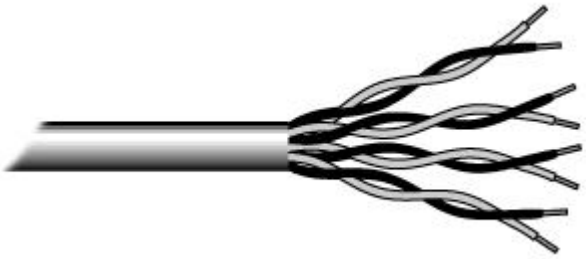
اتصال دهنده های فیبر نوری: SC,ST

کابل فیبر نوری با انواع مختلفی از کانکتورها می تواند کار کند، اما دو نوع معروفتر این کانکتورها یعنی ST(straight-tip) و SC(Subscriber) بیشتر موردتوجه قرار دارند. کانکتور ST برپایه BNC است با این تفاوت که بجای کابل مسی از فیبر نوری استفاده می شود. SC مربعی است و تا اندازه ای به Rj۴۵ شباهت دارد.

کابل فیبر نوری بدون توجه به نوع کانکتور در سرعتهای مشابه عمل میکند.

۱۰-۱-۲ : کابل UTP:

اگر از تلفن استفاده کرده باشید، کابل زوج به هم تابیده بدون پوشش برای شما آشناست - کابل UTP(Unshielded Twisted pair) 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.



شکل ۶-۲

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

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

:CAT۳

Cat۳یک درجه از کابل است که در شبکه بندی استفاده می شود ،اما cat۵بهتر از این نوع می باشد. نکته کلیدی درباره cat۳این است که این کابل هم اکنون در بیشتر ساختمانهای اداری و منازل وجود دارد . cat۳،کابل voice-gradeاست که در شبکه های تلفن از آن استفاده می شود.این کابل در شبکه هایی با حداکثر سرعت ۱۰Mbpsاستفاده می شود.

:CAT۵

بیشتر کابلهای utp در شبکه های امروزی cat۵ است.این کابل می تواند در شبکه هایی با حداکثر سرعت ۱۰۰Mbpsبکار گرفته شود.

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.

پیچیدگی بین وایرها به پوشش کابل برای جلوگیری از تداخلات الکترومغناطیسی کمک می کند.

کابل UTP از اتصال دهنده های پلاستیکی به نام RJ۴۵ استفاده می کند.این اتصال دهنده ها شبیه اتصال دهنده های تلفن می باشند با این تفاوت که در عوض ۴ وایری که در سیستم تلفن دیده می شود ، RJ۴۵ شبکه شامل ۸ اتصال می باشد .

نصب کابل UTP راحت تر از کواکسیال است زیرا به راحتی می توانید آن را در گوشه ها استفاده کنید .زوج به هم تابیده در مقابل نویزها از کواکسیال حساس تر است و در محیطهایی شامل وسایل بزرگ الکتریکی و الکترونیکی نباید استفاده شود .

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

(Jack Registered:RJ)

شکل ۷-۲

کابل STP:

این کابل زوج به هم تابیده پوشش دار است .تفاوت این کابل با UTP در این است که STP از یک پوشش حفاظتی با کیفیت بسیار عالی استفاده می کند .بنابراین این کابل کمتر در معرض تداخلات الکتریکی قرار می گیرد و سرعت های بالاتر در مسیرهای طولانی تر از UTP را پشتیبانی می کند .برای درک بهتر انواع کابل و اینکه چه موقع از هر کدام استفاده کنیم یک مثال در زیر آورده شده :

مثال :

یک شرکت دارای سه ساختمان یک اندازه می باش . هر کدام از این ساختمان ها ۴ طبقه دارند .اندازه هر ساختمان تقریبا ۲۰۰*۱۰۰ متر می باشد این شرکت به پهنای باند بالا وسرعت شبکه ۱۰۰Mbps نیاز دارد .

در نزدیکی این ساختمان ها یک ایستگاه رادیویی قرار دارد که سبب تداخلاتی روی همه وسایل و سیگنالهای الکتریکی محیط می شود .یکی از راه حلهای این مشکل در زیر آورده شده است:

۱ – ساختمان ها باید با کابل فیبر نوری به هم متصل شوند .

۲ – در طبقه بالایی هر ساختمان روتری قرار داده شود تا کابل های فیبر نوری را به هم متصل کند .

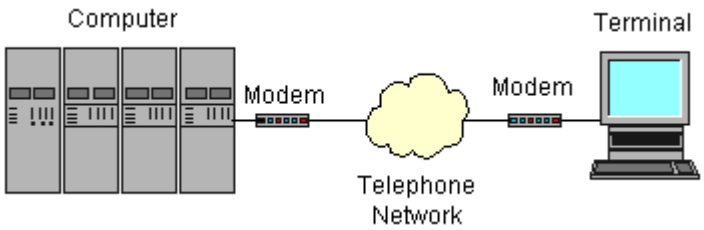
۳ – در هر طبقه از ساختمان ها با ید یک سوئیچ قرار دهیم که به روتر طبقه چهارم متصل شود .

۴ – در هر طبقه برای حذف تداخلات فرکانسهای رادیویی (RFI) که توسط ایستگاه رادیویی تولید می شود ،از کابل STP استفاده می کنیم .برای اتصال سوئیچ ها به روتر نیز از همین کابل استفاده می کنیم .

۲-۲: تولد مودم‌ها :

کلمه modem از اختصار کلمات modulator-demodulator گرفته شده است. یک مودم به صورت معمول یرای فرستادن اطلاعات دیجیتال روی خط تلفن استفاده می‌شود.مودم فرستنده، اطلاعات را به سیگنال‌های سازگار با خط تلفن تبدیل می‌کند، و مودم دریافت کننده، سیگنال را به اطلاعات دیجیتال برمی‌گرداند.

مودم‌ها در سال ۱۹۶۰ به عنوان یک راه برای اتصال ترمینال‌ها به رایانه‌ها روی خط تلفن، به وجود آمدند. یک شیوه معمول در زیر نشان داده شده است:



شکل ۸-۲

در یک شکل مثل این، یک terminal dumb در یک فروشگاه می‌توانست به یک رایانه مرکزی و بزرگ وصل شود. یک dumb terminal به صورت ساده یک کی‌برد و یک صفحه نمایش است. یک

dumb terminal خیلی رایج در آن زمان DEC VT-۱۰۰ نامیده شده بود و به عنوان استاندارد قرار گرفته بود. VT-۱۰۰ می‌توانست ۲۵ خط ۸۰ کاراکتری را نمایش دهد. وقتی کاربر یک کاراکتر در ترمینال وارد می‌کرد، مودم کد ASCII آن کاراکتر را به رایانه می‌فرستاد. بعد رایانه هم کاراکتر ها را به ترمینال برمی‌گرداند وآن‌ها هم، باید روی صفحه نمایش ظاهر می‌شدند.

وقتی رایانه‌های شخصی در اواخر ده ۷۰ میلادی شروع به ظهور کردند،(BBS(Bulletin-Board-Systems رایج شد.

یک نفر می‌توانست یک رایانه با یک مودم یا دو مودم و چندتا نرم افزار BBS راه اندازی کند و بقیه مردم برای اتصال به BBS شماره گیری می‌کردند. کاربران تقلید کننده‌های ترمینال را روی رایانه های خود برای تقلید یک dumb terminal اجرا می‌کردند.

مردم برای مدتی با ۳۰۰ بیت بر ثانیه راحت بودند. به این دلیل این سرعت قابل تحمل بود که ۳۰۰ bps حدود ۳۰ کاراکتر در ثانیه ارائه می‌کرد، که خیلی بیشتر از کاراکترهایی بود که یک نفر می‌تواند در ثانیه تایپ کند و یا بخواند. زمانی که مردم شروع به انتقال برنامه‌های بزرگ و تصویر به BBS و از آن کردند، bps۳۰۰ غیر قابل تحمل شد. مودم‌ها در سری‌های بعدی پیشرفت کردند:

۱۹۶۰۳۰۰ bps – تا ۱۹۸۳ یا بیشتر

۱۲۰۰ bps – در ۱۹۸۴ و ۱۹۸۵ رایج شد

۹۶۰۰ bps– در اواخر ۱۹۹۰ و اوایل ۱۹۹۱ ظاهر شد

kbps۱۹/۲

kbps۲۸/۸

kbps۳۳/۶

۵۶– kbps در سال ۱۹۹۸ استاندارد شد

– ADSL در تئوری به بیش از ۸ مگابیت بر ثانیه((Mbps می‌رسد – در سال ۱۹۹۹ رایج شد.

مودم‌های ۳۰۰ بیت بر ثانیه:

ما به دلیل سادگی از مودم‌های bps۳۰۰ به عنوان نقطه شروع استفاده می‌کنیم. مودم bps۳۰۰ یک دستگاهی است که از FSK(shift keying frequency) استفاده می‌کند. در FSK یک فرکانس(تن)جدا برای بیتهای مختلف مورد استفاده قرار می‌گیرد.

وقتی مودم یک ترمینال با مودم یک رایانه تماس می‌گیرد، مودم ترمینال، مودم مبدأ ((originate نامیده می‌شود، که آن یک تن ۱۰۷۰ هرتزی برای ۰(صفر) و یک تن ۱۲۷۰ هرتزی برای ۱(یک) می‌فرستد. مودم رایانه، مودم جواب((answer نامیده می‌شود و یک تن ۲۰۲۵ هرتزی برای ۰ (صفر) و یک تن ۲۲۲۵ هرتزی برای ۱(یک) می‌فرستد. به دلیل اینکه مودم جواب و مبدأ از فرکانس‌های مختلف استفاده می‌کنند به طور همزمان می‌توانند از خط استفاده کنند، که به عمل full-duplex معروف است. مودم‌های که می‌توانند فقط دریک زمان در یک مسیر اطلاعات را انتقال دهند به مودم‌های half-duplex معروف هستند، که کمیاب هستند.

اجازه بدهید که فرض کنیم دو مودم bps۳۰۰ به یکدیگر وصل شده‌اند، و کاربر در ترمینال حرف “a” را وارد می‌کند. کد ASCII برای این حرف ۹۷ در مبنای ۱۰ یا ۰۱۱۰۰۰۰۱ در مبنای ۲ است. یک دستگاه در ترمینال که UART(universal asynchronous receiver/transmitter) نامیده می‌شود این بایت را به بیت‌هایش تبدیل کرده و از پورت RS-۲۳۲ به بیرون می‌فرستد. مودم ترمینال به

درگاه RS-۲۳۲ متصل شده‌است، پس بیت‌ها را به ترتیب دریافت می‌کند و وظیفه‌اش فرستادن آن‌ها روی خط تلفن است.

مودم‌های سریعتر:

در امر ساخت مودم‌های سریعتر، طراحان مودم باید از روش‌های پیچیده‌تر از FSK استفاده می‌کردند. اول آنها به phase-shift keying)PSK) و بعد به quadrature amplitude modulation)QAM) دست پیدا کردند. این تکنیک‌ها اجازه می‌دهند که حجم غیر قابل باوری از اطلاعات به ۳۰۰۰ هرتز پهنای باند موجود در خط تلفن معمولی داده شود.

اینجا یک نگاه به درون مودم K۵۶ معمولی است:

شکل ۹-۲

همه این مودم‌های سرعت بالا دارای توانایی تنزل تدریجی((gradual degradation هستند، به این معنی که آن‌ها خط تلفن را آزمایش می‌کنند و اگر خط سرعتر های بالاتر مودم را جواب گو نباشد، به سرعت پایینتر برمی‌گردند.

قدم بعدی در انقلاب مودم‌ها، مودم‌های (asymmetric digital subscriber line(ADSL بودند. کلمه (asymmetricغیر متقارن) استفاده می‌شود، چون این مودم‌ها اطلاعات را در یک جهت با سرعت بیشتری نسبت به جهت دیگر ارسال می‌کنند. یک مودم ADSL از این حقیقت بهره می‌برد که هر خانه معمولی، آپارتمان یا اداره دارای یک سیم مسی اختصاصی است که بین آن و نزدیکترین مرکز یا اداره مرکزی تلفن، وجود دارد. این سیم مسی اختصاصی می‌تواند اطلاعاتی بیشتر از سیگنال ۳۰۰۰هرتزی که برای کانال صدای تلفن شما مورد نیاز است را ، انتقال دهد. اگر اداره مرکزی شرکت تلفن و خانه شما به مودم ADSL روی خط شما مجهز شده باشند، قسمت سیم مسی بین خانه شما و اداره تلفن می‌تواند به‌کلی به عنوان یک کانال ارتباطی دیجیتالی سرعت بالا عمل کند. ظرفیت، یک چیزی در حدود یک میلیون بیت بر ثانیه بین خانه شما و شرکت تلفن(که به این جهت upstream گفته می‌شود)، و۸ Mbps بین شرکت تلفن و خانه شما ((downstream در شرایط آرمانی است. در این حالت یک خط می‌تواند هم یک مکالمه تلفنی و هم اطلاعات دیجیتال را انتقال دهد.

روشی که مودم ADSL استفاده می‌کند در مفهوم بسار ساده است. پهنای باند خط تلفن بین ۲۴۰۰هرتز و ۱۱۰۰۰۰۰هرتز است، که به باندهای ۴۰۰۰هرتزی تقسیم می‌شود، و یک مودم مجازی به هر باند اختصاص داده می‌شود. هر کدام از این ۲۴۹ مودم مجازی به وجو آمده باندش را امتحان می‌کند و بهترین اسنفاده را از آن قسمت از پهنای باند گرفته را می‌برد.مجموع ۲۴۹ مودم مجازی سرعت کل مسیر را به وجود می‌آورد.

پروتکل Point-to-Point:

امروزه کسی از dumb terminal برای اتصال به یک رایانه جدا استفاده نمی‌کند. در عوض، ما از مودم‌ها برای اتصال به ISP ها استفاده می‌کنیم، و ISP ها ما را به اینترنت متصل می‌کنند. اینترنت هم به ما جازه می‌دهد تا به هر سیستمی در دنیا وصل بشویم. به دلیل نوع ارتباط رایانه شما، ISP و اینترنت، فرستادن تک کاراکترها، مناسب نیست. در عوض، مودم شما بسته‌های TCP/IP را بین شما وISP تان منتقل می کند .

تکنیک استاندارد برای فرستادن این بسته‌ها از مودمتان(Point-to-Point Protocol(PPP نامیده می‌شود. برای اطلاعات بیشتر در مورد پروتکل‌ها می‌توانید از لینک های و یا مقاله‌ها و آموزش‌های دیگر این سایت استفاده نمایید.

تکنولوژی های انتقالی :

FSK(Frequency Shift Keying)تکنیک مودمهای قدیمی : انتخاب فرکانسهای مختلف برای کاراکترهای مختلف با توجه به کد اسکی ASCII آنها. در FSK از یک فرکانس (tone) متفاوت برای بیت های متفاوت استفاده می گردید. زمانیکه یک مودم متصل به ترمینال با مودم متصل به کامپیوتر تماس می گرفت، مودم متصل به ترمینال مودم، originate نامیده می شود. مودم فوق برای مقدار" صفر" ، فرکانس ۱۰۷۰ هرتز و برای مقدار" یک"، فرکانس ۱۲۷۰ هرتز را ارسال می نماید. مودم متصل به کامپیوتر را مودم Answer می نامند. مودم فوق برای ارسال مقدار" صفر" ، فرکانس ۲۰۲۵ هرتز و برای مقدار" یک" ، فرکانس ۲۲۲۵ هرتز را ارسال می کرد.با توجه به اینکه مودم های فرستنده و گیرنده از فرکانس های متفاوت برای ارسال اطلاعات استفاده می کردند، امکان استفاده از خط بصورت همزمان فراهم می گردید. عملیات فوق Full-duplex نامیده می شود. مودم هائی که صرفا" قادر به ارسال اطلاعات در یک جهت در هر لحظه می باشند half-duplex نامیده می شوند. دستگاهی با نام UART موجود در ترمینال بایت ها را به بیت تبدیل و آنها را از طریق پورت سریال (RS-۲۳۲ Port) در هر لحظه ارسال می دارد.

·PSK (Phase Shift Keying) برتر از تکنولوژی منسوخ FSK. انتقال اطلاعات در این مودمها بر پایه ایجاد اختلاف فاز در سیگنال ارسالی بر حسب کدهای اسکی ASCIIمیباشد.

ADSL(line Asymmetric digital subscriber هر منزل و یا محل کار دارای یک کابل مسی اختصاصی بین محل مورد نظر و شرکت مخابرات مربوطه می باشد.ADSL قادر به حمل حجم بالائی از داده نسبت به سیگنال ۳۰۰۰ هرتزی مورد نیاز برای کانال های صوتی تلفن می باشد

بررسی لایه فیزیکی مودمها:

اساس ساختمان یک مودم:

۱.منبع تغذیه : وظیفه » تهیه ولتاژ مطلوب مورد نظر برای مدارات

۲.واحد فرستنده : شامل

الف : مدولاتور (تلفیق کننده) : تبدیل اطلاعات و داده های دیجیتالی به سیگنالهای آنالوگ.

ب: مدارات فیلتر ، ترکیب امواج و اضافه نمودن بیتهای کنترلی به سیگنالهای دیجیالی حاوی داده ها در هنگام ارسال.

۳.واحد گیرنده : شامل دمدولاتور (تجزیه کننده) میباشد.سیگنالهای آنالوگ را دریافت و در واحد پردازش مدولاسیون(تلفیق) آنها را پردازش و داده های دجیتالی اصلی را بر میگرداند.

مودم به شبکه تلفن سوئیچینگ عمومی(PSTN) وصل میشود.

رابطهای اصلی اتصال مودم :

- RS-۲۳۲-Cرابط ۲۵ پین . مودمهای قدیمی
- RS۲۳۲رابط ۹ پین ، مودمهای قدیمی

- رابط سریال Com۴ , Com۳ مودمهای داخلی Internalامروزی (همان سطح Rs۲۳۲ میباشند)
- رابط USB مودمهای خارجی (External) امروزی . سرعت بهتر. کیفیت و رفع خطای بیشتر و قطع ارتباط کمتر.

عملیات Multiplex:

شیوه ای از به اشتراک گزاری کانالهای اطلاعاتی میان کاربران. ایجاد فاصله های زمانی خاص میان کاربران.

روش مدولاسیون بایتی:

در این روش از ترکیب فرکانسها، دامنه آنها و شیفت دهی فاز سیکنالها استفاده میشود. اینروش در مودمهای مدرن امروزی جایگاه خاصی دارد. در مودمهای قدیمی فقط تغییر فرکانس در مدولاسیون صورت میگرفته.

لایه ارتباط داده ها در مودمها :

- شفاف سازی داده ها : انباشت و ارسال زنجیره ای داده ها در قالبها و قابهای مشخص.
- ارسال داده ها: قابلیت Full-Duplex(ارسال و دریافت مضاعف دوطرفه).
- کشف و تصحیح خطا : قابلیت CRC (Cyclical Redundancy Check) تست نسخه پشتیبان چرخشی. وارسی خطای N بیت،N بیت داده ها که N از حد اکثر طول رشته خطا بیشتر است. روش دوم روش کنترل اعشار X-ON / X-OFF است که بر مبنای کدهای ASCII میباشد.

- فشرده سازی داده ها / کد نمایی : تمام مودمهای جدید از یک شیوه استاندارد و مشترک برای فشرده سازی و کد / دکد نمودن بر مبنای کدهای ASCII تبعیت میکنند.

انواع استانداردهای مودمها :

۱. V.۲۲ فراهم سازی سرعت ۱۲۰۰ b/s با ۶۰۰ باود (Baud) «تغییر حالت در هر ثانیه»
۲. V.۲۲bis فراهم سازی سرعت ۲۴۰۰ b/s با ۶۰۰ باود (Baud)
۳. V.۳۲ فراهم سازی سرعت۴۸۰۰ b/s or ۴۸۰۰ b/s با ۶۰۰ باود (Baud)
٤. V.۳۲bis فراهم سازی سرعت ۱۹۶۰۰ b/s قابل تنظیم وکاهش.
۵. V.۳۴ فراهم سازی سرعت ۲۸۸۰۰ b/s و حمایت از استانداردهای V.۳۲ و V.۳۲bis
٦. V.۳۴bis فراهم سازی سرعت ۳۳۶۰۰ b/s
۷. V.۳۵ بدنه اصلی ارتباط شبکه های گسترده با شبکه های کوچک. ارتباط چندین خط تلفن به صورت گروهی.
۸. V.۴۲ حمایت از استانداردهای V.۳۲ و V.۳۲bis با این تمایز که کشف و تصحیح خطا در آن بهتر و پیچیده تر شده است.
۹. V.۹۰ فراهم سازی سرعت بال تر از۵۶۰۰۰ b/s قابل استفاده برای توپولوژی X۲ از ۳Com و نیز Rockwell K۵۶flex

مودم های کابلی:

در برخی از کشورهای دنیا نظیر امریکا سالیان متمادی است که مردم از تلویزیون های کابلی استفاده می نمایند. تنوع شبکه های تلویزیونی و کیفیت تصاویر از مهمترین دلایل گرایش مردم به تلویزیون های کابلی است . مشترکین تلویزیون های کابلی دارای یک گزینه مناسب جهت اتصال به اینترنت می باشند : مودم های کابلی . مودم های کابلی با تکنولوژی DSL رقابت می نمایند.

مبانی مودم های کابلی :

هر یک از سیگنال های تلویزیون در تلویزیون های کابلی دارای کانالی به اندازه ۶ مگاهرتز (شش میلیون سیکل در ثانیه) است. کابل های کواکسیال استفاده شده در تلویزیون های کابلی قادر به حمل صدها سیگنال مگاهرتزی می باشند. در سیستم تلویزیون های کابلی ، سیگنال های مربوط به هر کانال، پهنای باندی به اندازه ۶ مگاهرتز را اشغال می نمایند. در اغلب سیستم های فوق صرفا" از کابل کواکسیال استفاده می گردد. در سایر سیستم ها از فیبر نوری استفاده می گردد. ارسال سیگنا لها از طریق فیبر تا نزدیکترین ناحیه و یا محل ، انجام و در ادامه سیگنالهای مورد نظر با استفاده از کابل های کواکسیال به منزل مشترکین انتقال داده می شوند.

شرکت هائی که امکان دستیابی به اینترنت را از طریق کابل فراهم می نمایند ، قادر به ارسال اطلاعات و داده های اینترنت ازطریق کابل خواهند بود. علت این امر برخورد مودم های کابلی با داده ها بصورت downsteam است. (اطلاعات از اینترنت برای هر کامپیوتر و از طریق یک کانال ۶ مگاهرتزی ارسال می گردد) در زمان ارسال اطلاعات توسط کاربران ، هر یک از کاربران به پهنای باند بمراتب کمتری (دو مگاهرتز) نیاز خواهند داشت. بمنظور ارسال اطلاعات و دریافت اطلاعات کاربران از طریق مودم های کابلی به دو دستگاه خاص نیاز است : یک مودم کابلی(در محل مشترک)و یک "سیستم توقف مودم کابلی" Cable Modem termination system)(CMTS در محل شرکت ارائه دهنده خدمات .

اجزای یک مودم کابلی :

مودم های کابلی می توانند از نوع داخلی (Internal) و یا خارجی (External) باشند. مودم های کابلی دارای اجزای اساسی زیر می باشند :

- یک Tuner
- یک Demodulator
- یک Modulator
- یک دستگاه MAC(media access control)
- یک ریزپردازنده

در ادامه هر یک از اجزای فوق تشریح می گردد.

: Tuner

Tuner به کابل مربوطه متصل خواهد شد. در برخی حالات از یک Splitter (تقسیم کننده) بمنظور تفکیک کانال داده اینترنت از کانال های تلویزیونی استفاده می گردد. tuner سیگنال های مدوله شده دیجیتال را دریافت و آنها را در اختیار demodulator قرار می دهد. در برخی حالات tuner از یک diplexer استفاده می نماید. diplexer ، امکان استفاده tuner از یک مجموعه فرکانس ها (معمولا" بین ۴۲ و ۸۵۰ مگا هرتز) برای ترافیک downstream و مجموعه دیگر از فرکانس ها (معمولا" ۵ و ۴۲ مگاهرتز) را برای ترافیک upstream فراهم می نماید. در برخی از سیستم ها (در اغلب سیستم هائی که دارای محدودیت ظرفیت برای کانال می باشند) ، از tuner مودم کابلی برای داده های Downstream و از یک مودم معمولی (Dial-Up) برای ترافیک upstream استفاده می گردد. در هر یک از موارد فوق ، tuner پس از دریافت سیگنال ، آن را برای یک demodulator ارسال خواهد کرد.

: Demodulator

اکثر demodulator ها ، چهار عملیات اساسی را انجام می دهند . یک سیگنال رادیوئی (حاوی اطلاعات رمز شده با تغییر amplitude و phase) را بعنوان ورودی گرفته و آن را به یک سیگنال ساده قابل پردازش توسط یک "مبدل آنالوگ به دیجیتال " ، تبدیل می نماید. مبدل مربوطه پس از دریافت سیگنال (ولتاژ آن متغیر است) ، آن را به مجموعه ای از صفر و یک تبدیل می نماید. در فرآیند فوق از یک ماژول تصحیح کننده خطاء ، بمنظور بررسی صحت اطلاعات دریافت شده استفاده خواهد شد. بدین ترتیب در صورت بروز خطاء در ارسال اطلاعات ، امکان تشخیص و برخورد با آنان وجود خواهد داشت .

: Modulator

در مودم های کابلی که از سیستم کابل برای ترافیک upstream استفاده می نمایند،از یک modulator بمنظور تبدیل داده های دیجیتال به سیگنا ل های رادیوئی برای انتقال اطلاعات استفاده می شود. عنصر فوق از سه بخش مجزا تشکیل شده است :

- یک بخش بمنظور درج اطلاعات استفاده شده برای تصحیح خطاء
- یک QAM modulator
- یک مبدل دیجیتال به آنالوگ

: MAC

MAC بین بخش های Downstream و Upstream یک مودم کابلی قرار گرفته و بعنوان یک اینترفیس بین بخش های نرم افزاری و سخت افزاری ، پروتکل های متفاوت شبکه ها عمل می نماید. تمام دستگاههای شبکه دارای MAC می باشند. در مودم های کابلی با توجه به پیچیدگی موجود، سعی می گردد که برخی از عملیات مربوط به MAC توسط پردازنده اصلی مودم کابلی صورت پذیرد.

ریزپردازنده:

عملکرد ریزپردازنده بستگی به نوع انتظارات مربوطه از مودم های کابلی و نحوه تامین انتظارات دارد.در برخی موارد مودم کابلی خود بعنوان بخشی از یک سیستم کامپیوتری بزرگ بوده و یا ممکن است دستیابی به اینترنت بدون وساطت عناصر دیگر ، مستقیما" توسط مودم کابلی انجام گردد.

(CMTS)(Cable Modem termination system):

عملکرد CMTS در مودم های کابلی (تجهیزات نصب شده در شرکت ارائه دهنده خدمات فوق) ، مشابه DSLAM در DSL است . CMTS ، ترافیک مجموعه ای از مشترکین را اخذ و پس از استقرار در یک کانال ، آنها را برای مرکز ارائه دهنده خدمات اینترنت ((ISP ارسال می دارد. اطلاعات ارسال شده توسط ISP برای تمام مشترکین فرستاده خواهد شد. (نظیر شبکه های اترنت) . تشخیص اینکه اطلاعات ارسالی مربوط به کدامیک از مشترکین است برعهده تجهیزات استفاده شده در محل مشتری است . اطلاعاتی که توسط مشترکین برای CMTS ارسال می گردد ،توسط سایر مشترکین قابل مشاهده نخواهد بود. پهنای باند مربوطه برای ارسال اطلاعات مشترکین به مجموعه ای از واحدهای زمانی (بر حسب میلی ثانیه) تقسیم و هر یک از کاربران قادر به استفاده از پهنای باند فوق در یک مقطع زمانی پیوسته خواهند بود.

یک CMTS قادر به ارسال اطلاعات ۱.۰۰۰ کاربر اینترنت از طریق یک کانال ۶ مگاهرتزی است . هر کانال قادر به ارسال ۳۰ تا ۴۰ مگابیت در ثانیه است . بدین ترتیب کاربران دارای سرعت و کارآئی بمراتب بیشتر نسبت به مودم های معمولی می باشند.

در صورتیکه کاربری با استفاده از مودم کابلی به اینترنت متصل گردد (صرفا" کاربر فوق در لحظه مورد نظر به اینترنت متصل است) ، تمام پهنای باند موجود به وی اختصاص داده خواهد شد . بموازات ورود سایر کاربران به شبکه و یا انجام عملیات سنگین توسط برخی از کاربران ، سرعت و کارآئی هر یک از کاربران بمنظور دستیابی به اطلاعات افت خواهد کرد (پهنای باند بصورت مشترک بین تمام کاربران و بر اساس یک

الگوریتم زمانبندی خاص اختصاص داده می شود) در چنین مواردی ، شرکت های ارائه دهنده خدمات مودم کابلی می بایست یک کانال جدید را اضافه و با توزیع مناسب کاربران بر روی هر یک از کانال های موجود ، قادر به برطرف نمودن مشکل سرعت و کارآئی کاربران و مشترکین خود می باشند. کارآئی دستیابی به اینترنت با استفاده از مودم های کابلی بر خلاف خطوط ADSL ، به مسافت موجود بین مشترک و شرکت ارائه دهنده خدمات ، بستگی ندارد.

ارزیابی کیفیت مودمهای سری ۵۶k :

بر طبق قوانین FCC همه سازندگان مودم باید این فاکتورها را همراه مودم به خریدار ارائه دهند :

۱.محدودیت های پهنای باند

۲.میزان نویز پذیری در خطوط تلفن

۳.(تکنولوژی) مبدل دیجیتال به آنالوگ

۴.(تکنولوژی) مبدل آنالوگ به دیجیتال

۵.نوع و شیوه پردازشها و قالب بندی داده ها

اکنون به بررسی جزئیات میپردازیم:

۱. پهنای باند : پهنای باند خطوط تلفن ۳۰۰۰ هرتز است . این پهنای باند است که ظرفیت انتقال اطلاعات روی باند را به ما نشان میدهد.

bit rate = bandwidth*(log۲(۱ + S/N))

۵۳۰۰۰ bps = (۳۰۰۰ Hz)*(log۲(۱ + S/N))

so the S/N must be at least ۲۰۸۵۴۵. SNR = ۱۰ log(S/N) = ۵۳.۲ dB

۲. مبدل دیجیتال آنالوگ دیجیتال : با توجه به تکنولوژی مبدلهاست که میتوان فاکتورهای حیاتی ای از کیفیت مودم به دست آورد. مثلا میزان نویز پذیری مودم. در مودمها یک واحد بسیار مورد توجه است ، *Quantization noise* یا میزان پله ای کردن نویز :

quantization noise = (۱/۲^q)^۲

if signal = ۱, then S/N = ۲^۲q

۲^۲q = ۳۱۶۲.۳

q = ۵.۸۱ bits

۳. قالب بندی اطلاعات : پروتکل معروف PPP از فرمت قالب بندی HDLCاستفاده میکند.به جدول زیر نگاه کنید :

	Flag	Address	Control	Data	FCS	Flag
# of bits	۸	۸ or ۱۶	۸ or ۱۶	variable	۱۶ or ۳۲	۸

مودم :

- آسنکرون(آنالوگ) : پهنای باند کوتاه . روش ارتباطی یک طرفه.داده‌ها را در قالب یک جریان متناوب از بسته‌های داده‌ای کوچک ارسال می‌کند
- سنکرون : معمولا در محیط‌های leased-line مورد استفاده قرار می‌گیرند و در این تکنیک از مالتی پلکسرها برای برقراری ارتباط بین ترمینالها و سرورها و کامپیوترهای mainframe استفاده می‌گردد

اینترنت بدون کابل : در سال ۱۹۹۷ ، شرکت های نوکیا ، موتورولا ، اریکسون و Phone.com ، پروتکل (Wireless Application Protocol) WAP را ایجاد کردند. هدف از پروتکل فوق ارائه استاندارد لازم بمنظور پیاده سازی اینترنت بدون کابل بود.

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 بهbroadband بود (مودم های کابلی و خطوط DSL) .

مقایسه انواع DSL :

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

- ADSL(DSL Asymmetric) . 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(DSL High bit-rate) . سرعت مدل فوق در حد خطوط T۱ است (۵/۱ مگابیت در ثانیه) .سرعت دریافت و ارسال اطلاعا ت در روش فوق یکسان بوده و بمنظور ارائه خدمات نیاز به دو خط مجزا نسبت به خط تلفن معمولی موجود است .
- ISDL(DSL ISDN) . 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 ۱۴۴ کیلوبیت در ثانیه است (دو جهت) .
- MSDSL(DSL Multirate Symmetric) . در مدل فوق سرعت ارسال و دریافت اطلاعات یکسان است . نرخ سرعت انتقال اطلاعات توسط مرکز ارائه دهنده سرویس DSL ، تنظیم می گردد.
- RADSL(Adaptive Rate) . 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(DSL Symmetric) . 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(bit-rate Very high) . مدل فوق بصورت "نامتقارن " بوده و در مسافت های کوتاه بهمراه خطوط مسی تلفن استفاده می گردد.
- VoDSL(DSL Voice-over) . یک نوع خاص از IP تلفنی است . در مدل فوق چندین خط تلفن ترکیب و به یک خط تلفن تبدیل تبدیل می شوند.

۳-۲ : کارت شبکه :

از نظر سخت افزاری دو نوع کارت شبکه داریم :

- کارت NIC که برای LAN استفاده میشود.
- Modem که در شبکه های ون بکار می رود .

نقش کارت شبکه :

کارت شبکه به عنوان رابطه فیزیکی یا اتصال بین کامپیوترکابل شبکه عمل میکند این کارت ها در هر یک از Slot های کامپیوترقابل نصب اند. بعد از نصب کارت شبکه، کابل شبکه به درگاه کارت متصل شده و ارتباط فیزیکی واقعی بین کامپیوتر و باقی شبکه برقرارمیشود.

وظایف کارت شبکه :

- ارسال داده ها به کامپیوتر دیگر.
- دریافت داده ها .
- کنترل جریان داده ها میان کامپیوتروسیم کابل کشی .

کارت شبکه شامل سخت افزار ومیان افزارFirmwave است میان افزار به روتین های نرم افزاری که در حافظه Rom ذخیره می شو ند، می گویند .

ارسال : اطلاعاتی که از کامپیوتر وارد کارت میشود، به صورت موازی اند. این اطلاعات برای انتقال از طریق سیم باید به صورت سری تبدیل شوند این عمل را کارت شبکه انجام میدهد .

دریافت : اطلاعات از سیم به صورت سری دریافت میشود کارت شبکه آنها را به صورت موازی تبدیل کرده و به کامپیوتر ارسال میکند

.

کنترل : در زمان ارسال ودریافت اطلاعات باید یکسری اطلاعات کنترلی رد و بدل شوند. ارسال این اطلاعات کنترلی را کارت شبکه برعهده دارد.

ترنسیور: بخشی از کارت است که عمل تبدیل اطلاعات سری به موازی را به عهده دارد

اطلاعاتی که در زمان کنترل ارسال میشود:

۱-حداکثر اندازه بسته ای که ارسال میشود چقدر است.

۲-حجم اطلاعات کنترلی چقدر است .

۳-فواصل زمانی میان ارسال هر بسته چقدر است .

۴-مدت زمانی که باید منتظر جواب برگشت (Ack) باشد.

۵-حجم اطلاعاتی که هر کارت میتواند قبل از سر ریز شد ن درخود نگه دارد.

۶-سرعت ارسال داده ها .

روی کارت شبکه chipsetهای گوناگون وجود دارد وظیفه قسمت کنترل توسط این chipsedهاتعیین میشود.

آدرس دهی سخت افزاری ونرم افزاری:

هر کامپیوتر برای آنکه در شبکه شناسایی شود نیاز به آدرسی دارد. درسیستم عامل ناول برای کامپیوتر نامی اختصاص میداند ولی امروزه علاوه به نام، عدد منحصر به فردی نیز بدهد کامپیوتراختصاص داده میشود.

آدرسی که در حافظه bios کارت شبکه ثبت میشود آدرس سخت افزار کارت شبکه نام دارد. این آدرس سخت افزاری منحصر به خود است، ولی کار با این آدرس مشکل است لذا برای هر کامپیوتر نامی تعیین میشود درTCP/IPهرsewer یک URL دارد ولی علاوه بر URL یک آدرس IPهم وجود دارد.آدر IP وURL آدرس های نرم افزاری اند.

سرعت های مختلف کارت :

کارت های رایج امروزی سرعت های۱۰/ ۱۰۰ Mb/p را دارند .

امروزه سرعت های۱۰۰۰ /۱۰۰/ ۱۰ هم وجود دارد.

روی کارت ها LED هایی وجود دارد مثلا در زمان اتصال به HUB، لامپ ACT روشن می شود که نشان می دهد تمام ارتباطات تا Hub درست می باشد. در بعضی کارتها چشمک زدن Actنشان دهنده تبادل اطلاعات می باشد.

پیکربندی سخت افزاری و نرم افزاری:

کارت های شبکه قدیمی یکسری Jumper داشتند که تنظیمات آنها از طریق این Jumper ها انجام می شد. کارت های امروزی Jumperless اند یعنی به صورت Plug and play عمل می کنند و نیازی به تنظیم توسط کاربر ندارند و توسط سیستم عامل تشخیص داده شده و کار می کنند. به عمل تنظیم این Jumperها Setting گفته می شود. در نمونه های جدید کارت به جای Jumper از D.S استفاده می شود که دو حالت ON و OFF دارند .

خطوط درخواست وقفه (IRQ)

خطوط درخواست وقفه، خطوط سخت افزاری هستند که وسایلی مانند درگاههای I/O، صفحه کلید، کارت شبکه و ... می توانند وقفه درخواست خود را برای سرویس گرفتن از میکرو پروسسور کامپیوتر از طریق آن ارسال کنند. وقتی کارت شبکه یک درخواست به کامپیوتر می فرستد از یک وقفه استفاده می کند یعنی یک سیگنال الکترونیکی به CPU کامپیوتر می فرستد.در اغلب موارد IRQ۳ وIRQ۵ برای کارت شبکه مورد استفاده قرار می گیرد. به طور پیش فرض IRQ۵ برای کارت شبکه استفاده می شود.

نرم افزار MSD (Microsoft Director):

برای اطلاع از اینکه کدام یک از IRQ ها آزاد هستند از این نرم افزار استفاده می شود.

آدرس پایه I/O (Base I/O Address):

کانالی که اطلاعات از طریق آن بین سخت افزار کامپیوتر (کارت شبکه) و CPU مبادله می شود این درگاه از دید CPU یک آدرس است.شماره درگاه پیش فرض کارت شبکه ۳۰۰-۳۰F(H) یا ۳۱۰-۳۱F (H) است.

آدرس حافظه پایه Base memory :

آدرس حافظه پایه، محلی را در حافظه کامپیوتر RAM مشخص می کند که توسط کارت شبکه به عنوان بافر برای ذخیره موقت بسته های اطلاعاتی دریافتی و ارسال مورد استفاده قرار می گیرد.آدرس حافظه پایه برای کارت شبکه اغلب D۸۰۰۰ است.بعضی از کارت ها دارای بافر هستند که این بافر به حجم حافظه آنها اضافه می شود.

اصطلاح Direct memory Access DMA (دسترسی مستقیم به حافظه):

به عمل دسترسی مستقیم به حافظه بدون در نظارت CPU گفته می شود. در این روش داده ها مستقیما از بافر کارت شبکه به حافظه کامپیوتر انتقال می یابد و از ریزپردازنده کامپیوتر استفاده نمی شود.

انواع پورت های کارت شبکه :

۱- پورت ذوزنقه ای یا پورت AUI یاDIX که یک رابط ۱۵ سوزنه است و از قوانین ۱۰base۵ استفاده می کند و با کابل coaxial ضخیم بکار می رود.

۲- پورت دایره ای شکل یا پورت BNC که از قانون ۱۰base۲ و کابل Coaxial نازک استفاده می شود.

۳- پورت مربعی شکل یا پورت Rj۴۵ که از قانون ۱۰baseT استفاده و با کابل UTP Cat۵/cat۳ بکار می رود.

انواع کارت شبکه بر اساس نوع Slot :

Slot های کامپیوترهای شخصی دارای چهار نوع معماری می باشند.

- ISA

- EISA

- MCA

- PCI

ISA:

قدیمی ترین نوع کارت شبکه از نوع ISA هستند. ISA های اولیه ۸ بیتی بودند و سرعت آنها MB۱۰ می باشد. در سال ۱۹۸۴،ISAهای ۱۶ بیتی ایجاد شدند که شکاف های آنها دو شکاف پشت سر هم بود.

EISA :

EISA یک گذرگاه ۳۲ بیتی برای انتقال داده است.

MCA :

معماری MCA ازنظر فیزیکی و الکترونیکی با گذرگاه ISA ناسازگار است.

PCI :

یک گذرگاه ۳۲ بیتی است که امروزه از این نوع کارتها استفاده می شود که دارای سرعت ۱۰۰/۱۰ MBit اند.

BOOTROM:

در تمام کارت های شبکه یک مکان خالی IC وجود دارد که ۲۸ پایه دارد این مکان، جای BootRom است.در برخی محیط ها، امنیت شبکه آنقدر اهمیت دارد که از دیسک درایو در دستگاهای کاری استفاده نمی شود. بدون دیسک درایو کاربران نمی توانند اطلاعات را از دیسک و یا به دیسک سخت کپی کنند

بنابراین نمی توان هیچ دادهای از سایت شبکه خارج نمایند. در کامپیوترهایی که دیسک سخت وجود دندارد از یک تراشه به نام بوت رام برای بوت کردن کامپیوتر استفاده می شود که بعد از بوت شدن به شبکه متصل شود که اصطلاحا Disckless نام دارد. برای تنظیم بوت رام جامپرهایی وجود دارد که حالت Disable و Enable دارند ولی امروزه این تنظیمات نرم افزاری انجام می شود.

چند مشخصه مهم یک کارت :

۱- مارک Chipset و نام آن: اساسی ترین مشخصه روی کارت شبکه است.

۲- استاندارد: کارت ها دارای چه استانداردی هستند ۱۰baset و ۱۰base۲ و ۱۰۰basetx

۳- Base I/O Address

۴- سرعت انتقال data transmition

۵- کابل های ارتباط Cable Connections

۶- Ledهای روی کارت

۷- Bus Interface

۸- Wake on lan قابلیت خواب و بیداری

۹- قابلیتی است که کامپیوتر می تواند در حالت standby باشد زمانی که پکت می رسد از حالت Standby خارج شده و پکت را دریافت و دوباره به حالت Standby رود.

۱. روتر
۲. نحوه ارسال پیام
۳. ارسال بسته های اطلاعاتی
٤. آگاهی از مقصد یک پیام
٥. پروتکل ها
٦. ردیابی یک پیام
۷. ستون فقرات اینترنت

۲-۴ : 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.

بمنظور 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 بمنظور 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 سایر کاربران سازمان در نظر گرفته می شود. بمنظور ارتباط 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 صورتیکه 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 بعنوان 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 بمنظور 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 صورتیکه 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 بعنوان 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 بمنظور 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. بمنظور ارتباط روتر به مرکز ارائه دهنده خدمات اینترنت ((ISP می توان از خطوط اختصاصی با سرعت های متفاوت استفاده کرد. خط اختصاصی T۱ 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 بمنظور ارتباط روتر با ISP استفاده نمایند. خط فوق بصورت Backup بوده و بمحض بروز اشکال در خط اختصاصی (مثلا" T۱) 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 تر را 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 بمنظور اعمال سیاست های امنیتی می باشند. قوانین 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 صورتیکه بسته اطلاعاتی مربوط به شبکه داخلی بوده نیازی به روت نمودن آن توسط روتر نخواهد بود. بدین 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. بمنظور انجام عملیات فوق ، روترها می بایست نسبت به دو موضوع آگاهی داشته باشند : آدرس ها و ساختار شبکه

.

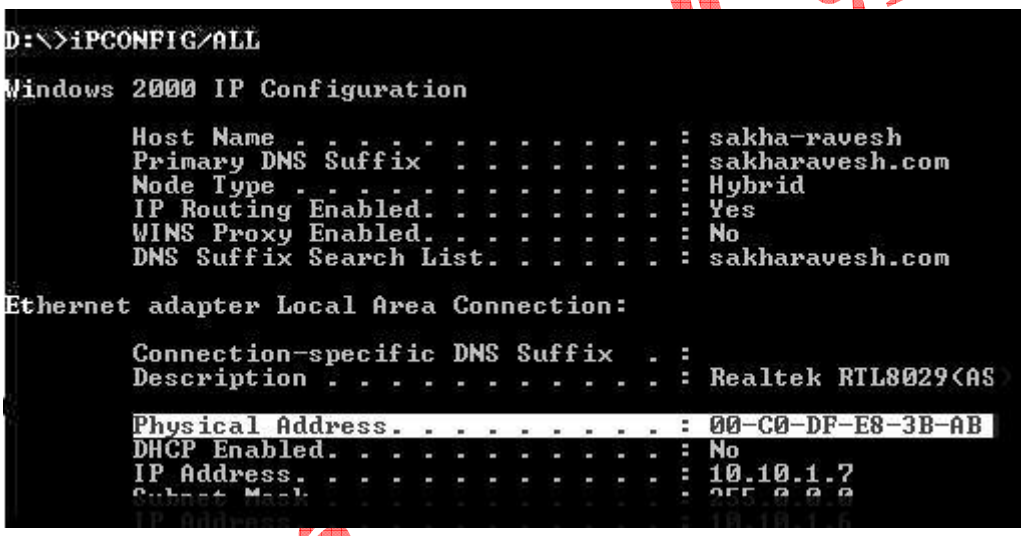
زمانیکه توسط یکی از دوستانتان برای شما یک کارت تبریک سال نو ارسال می گردد ، از آدرسی مطابق زیر استفاده می نماید : " تهران - خیابان ایران - کوچه شمیرانات - پلاک ۱۱۰ " آدرس فوق دارای چندین بخش بوده که به اداره پست مربوطه امکان پیدا نمودن آدرس فوق را خواهد داد. استفاده از کد پستی باعث سرعت در ارسال کارت تبریک و دریافت آن توسط شخص مورد نظر می نماید .ولی حتی در صورتیکه 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 صورتیکه 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 در رابطه 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 صورتیکه 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 بمنظور 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 بعنوان 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 مجددا" 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 Packet-Switched network 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 صورتیکه از سیستم عامل ویندوز استفاده می نمائید ، با استفاده از دستور Traceroute می توانید مسیر بسته های اطلاعاتی را دنبال نمائید. مثلا" در صورتیکه بخواهیم از مسیر پیوستن به سایت http://www.microsoft.com/ آگاهی پیدا نمائیم ، کافی است دستور فوق را بصورت زیر تایپ نمائیم :

Tracert http://www.microsoft.com/

اولین اعداد نشاندهنده تعداد روترموجود بین کامپیوتر شما و سایت مایکروسافت است . در این مدل خاص از روتر استفاده شده است . سه عدد بعدی ، نشاندهنده مدت زمانی است که اطلاعات از کامپیوتر شما برای روتر (مشخص شده) ارسال و مجددا" مراجعت می نمایند. در برخی موارد ممکن است نام روتر نیز اعلام گردد. در نهایت آدرس IP هر یک از روترها نشان داده شده است .بدین ترتیب برای رسیدن به

سایت مایکروسافت از محلی که دستور فوق تایپ می گردد ، .... روتر استفاده و ثانیه زمان برای دریافت اطلاعات از سرویس دهنده و مراجعت مجدد اطلاعات ، نیاز خواهد بود.

ستون فقرات اینترنت :

باتوجه به گستردگی اینترنت و وجود میلیون ها بسته اطلاعاتی در هر ثانیه بمنظور مسیریابی ، می بایست از روترهای با سرعت بالا استفاده شود. روتر سری ۱۲۰۰۰ سیسکو یکی از این نوع روترها بوده که بعنوان 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 MHZ MIPS R۵۰۰۰۲۰۰ 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 صورتیکه مدل فوق با تمام توان و ظرفیت خود نصب گردد ، امکان انتقال ۶۰ میلیون بسته اطلاعاتی در هر ثانیه 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 صورتیکه مسیر فوق فاقد کارآئی لازم باشد ، روتر مسیر فوق را چشم پوشی نموده و مجددا" 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 صرفا" 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، صرفا" عملیات فوق را انجام داده و برخی دیگر از روترها عملیات بمراتب بیشتر و پیچیده تری را

انجام می دهند.

سوئیچ
استفاده از سوئیچ
تکنولوژی سوئیچ ها
Bridging Transparent
فراوانی و آشفتگی انتشار
tress Spanning
روترها و سوئیچینگ لایه سوم

۵-۲ : 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.

استفاده از سوئیچ :

در اکثر شبکه های متداول ، بمنظور 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 بمنظور 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 صورتیکه یکی از کاربران فایل با ظرفیت بالائی را برای کاربر دیگر ارسال نماید ، تمام کاربران دیگر می بایست در انتظاز آزاد شدن محیط انتقال بمنظور ارسال اطلاعات باشند. بهرحال افزایش مدت زمانی که یک بسته اطلاعاتی به مقصد خود برسد ، هرگز مورد نظر کاربران یک شبکه نخواهد بود.

- Network Failure . 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 بمنظور ارتباط در شبکه استفاده می گردد. فرآیند فوق نحوه استفاده از محیط انتقال بمنظور 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 صورتیکه 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 بمنظور 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 صورتیکه یک دستگاه متصل شده به سوئیچ ، دارای تمام پهنای باند مختص خود است. مثلا" در صورتیکه 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 صورتیکه سایر گره ها نیز قصد ارتباط را داشته باشند) . در سوئیچ ، هر یک از گره ها قادر به برقراری ارتباط با سایر گره 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 و گره 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.

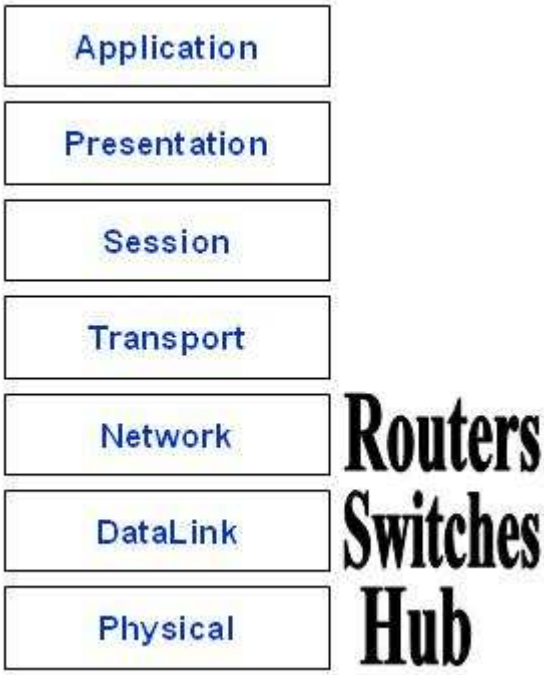
در شبکه های مبتنی بر سوئیچ امکان استفاده از کابل های بهم تابیده و یا فیبر نوری وجود خواهد داشت . هر یک از کابل های فوق دارای کانکتورهای مربوط به خود برای ارسال و دریافت اطلاعات می باشند. با استفاده از سوئیچ ، شبکه ای عاری از تصادم اطلاعاتی بوجود خواهد آمد. انتقال دو سویه اطلاعات در شبکه های مبتنی بر سوئیچ ، 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 بمنظور 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 بمنظور 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

استفاده می شود. (آدرس ها ی منطقی) . الگوریتم استفاده شده توسط سوئیچ بمنظور اتخاذ تصمیم در رابطه با مقصد یک بسته اطلاعاتی با الگوریتم استفاده شده توسط روتر ، متفاوت است .



شکل ۲-۱۰

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 صورتیکه 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 بمنظور 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 صورتیکه 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 ۶۴ 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.

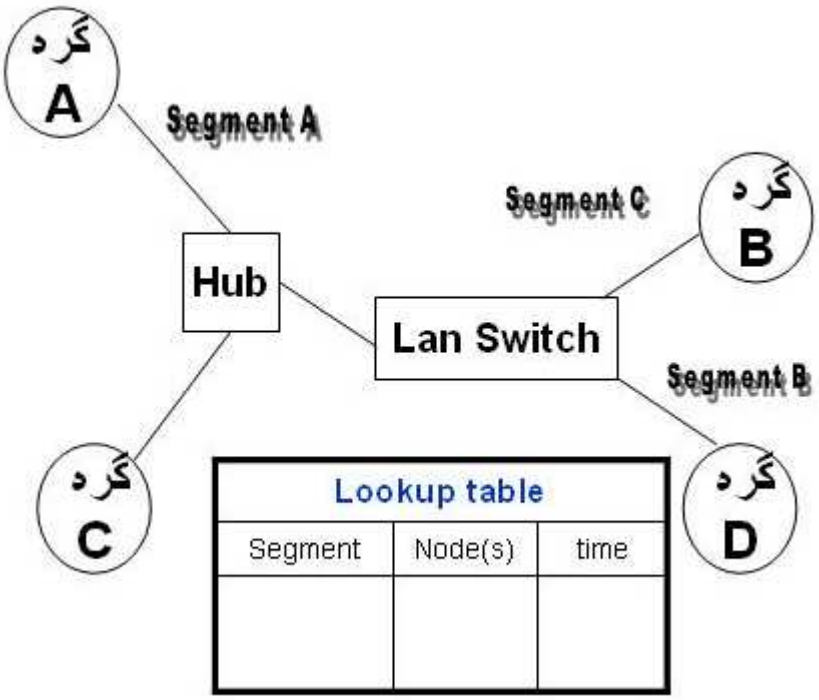
-Matrix . این نوع از سوئیچ ها دارای یک شبکه(تور) داخلی ماتریس مانند بوده که پورت های ورودی و خروجی همدیگر را قطع می نمایند. زمانیکه یک بسته اطلاعاتی بر روی پورت ورودی تشخیص داده شد ، آدرس MAC آن با جدول lookup مقایسه تا پورت مورد نظر خروجی آن مشخص گردد. در ادامه سوئیچ یک ارتباط را از طریق شبکه و در محلی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

- Bus Architecture . 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.

Bridging Transparent :

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



شکل ۱۱-۲

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 دیگر (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 ، بمنظور یافتن یک گره خاص برای تمام سگمنت ها ، Flooding نامیده می شود.

- گره B بسته اطلاعاتی را دریافت و یک بسته اطلاعاتی را بعنوان 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 بمنظور ارسال بسته اطلاعاتی دو سگمنت را به یکدیگر متصل نمائید. فرآیند فوق Forwarding نامیده می شود.

- در ادامه بسته اطلاعاتی بعدی از گره A بمنظور 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 بمنظور 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.

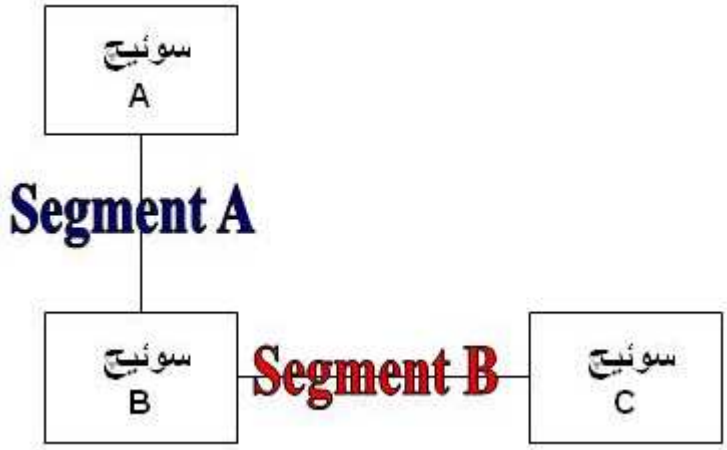
- Learning و Flooding ادامه یافته و بموازات آن سوئیچ ، آدرس های MAC مربوط به گره ها را در جداول Lookup ذخیره می نماید. اکثر سوئیچ ها دارای حافظه کافی بمنظور ذخیره سازی جداول

Lookup می باشند. بمنظور 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 ، هر گره دارای سگمنت اختصاصی مربوط بخود است . بدین ترتیب امکان تصادم حذف و نیازی به عملیات Filtering نخواهد بود.

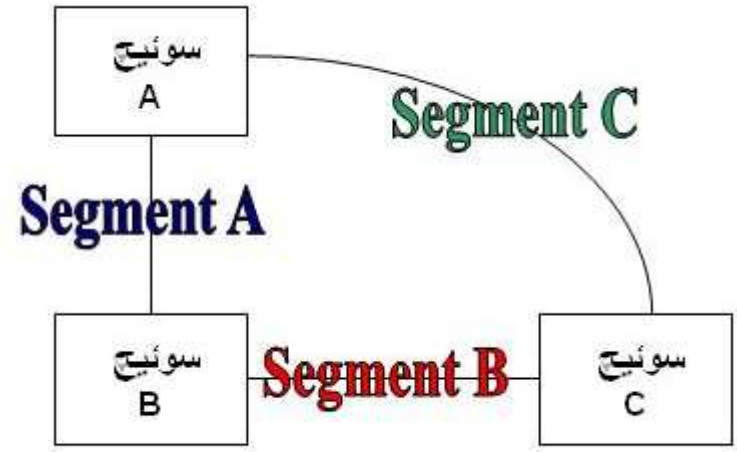
فراوانی و آشفتگی انتشار:

در شبکه های با توپولوژی ستاره (Star) و یا ترکیب Bus و Star 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 :



شکل ۱۲-۲

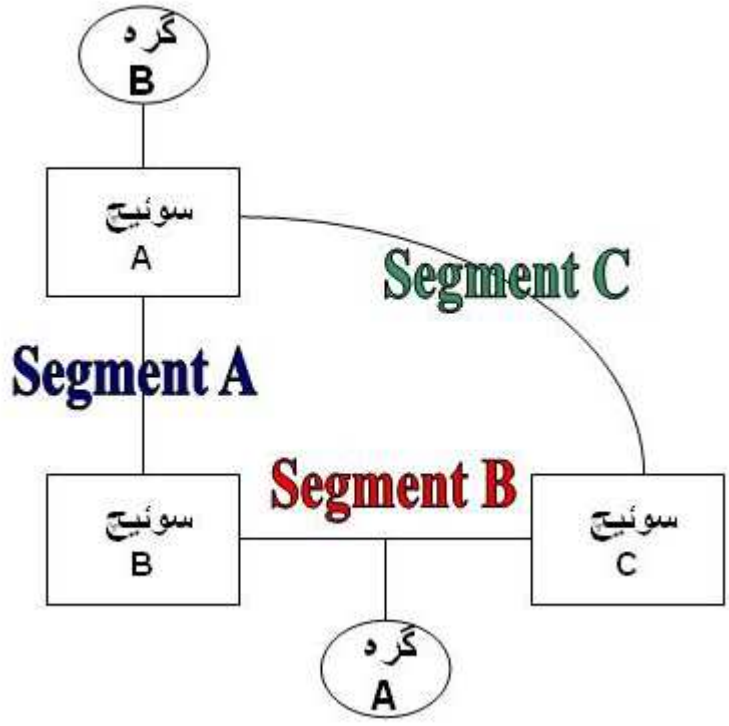
در مثال فوق ، در صورتیکه سوئیچ A و یا C با مشکل مواجه گردند، تمام گره های متصل به هر یک از سوئیچ های فوق نیز تحت تاثیر اشکال فوق قرار خواهند گرفت . گره های متصل به سوئیچ دیگر ((B کماکن قادر به ارائه خدمات خود خواهد بود. در صورتیکه سوئیچ C با اشکال مواجه گردد ، تمام شبکه از کار خواهد افتاد . در صورت اضافه کردن سگمنت دیگر برای ارتباط سوئیچ A و C چه اتفاقی خواهد افتاد .



شکل ۱۳-۲

در حالت فوق ، در صورتیکه یکی از سوئیچ ها با اشکال مواجه گردد ، شبکه کماکن قادر به ارائه خدمات خود خواهد 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.



شکل ۱۴-۲

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 اضافه می نماید. (برای سگمنت A) . سوئیچ C آدرس گره B را بمنظور 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.

tress Spanning :

بمنظوری 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 بمنظور مشخص نمودن اولویت و شش بایت برای مشخص

کردن آدرس MAC استفاده می گردد. مشخصه پورت ها ، شانزده بیتی است . شش بیت بمنظور 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 . بمنظور 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) . بمنظور 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 Path cost می تواند یک مقدار دلخواه بوده که توسط مدیریت شبکه تعریف و مشخص می گردد)

STP Cost Value	Bandwidth
۲۵۰	۴ Mbps
۱۰۰	۱۰ Mbps
۶۲	۱۶ Mbps
۳۹	۴۵ Mbps
۱۹	۱۰۰ Mbps
۱۴	۱۵۵ Mbps

۶	۶۲۲ Mbps
۴	۱ Gbps
۲	۱۰ Gbps

- هر سوئیچ فرآیندی را بمنظور 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 BPUDبشرح 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. مثلا" در صورتیکه 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 بمنظور 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 بمنظور 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 بعنوان Root در نظر می گیرد. زمانیکه یک سوئیچ برای اولین بار به شبکه متصل می گردد ، یک BPDU را بهمراه BID خود که بعنوان Root BID است ، ارسال می نماید. زمانیکه سایر سوئیچ ها BPDU را دریافت می دارند ، آن را با BID مربوطه ای که بعنوان BID Root ذخیره نموده اند، مقایسه می نمایند. در صورتیکه BID Root جدید دارای یک مقدار کمتر باشد ، تمام سوئیچ ها آن را با آنچیزی که قبلا" ذخیره کرده اند، جایگزین می نمایند. در صورتیکه BID Root 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 بعنوان 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 Root Bridge است . پورت های فوق، Ports Root 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 برای path cost است ، هر پورت آن بمنزله 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 صورتیکه پورتی دارای پایین ترین path cost باشد ، پورت فوق بمنزله پورت designated سگمنت مورد نظر خواهد بود. در صورتیکه 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 بعنوان port non -designated 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 . (Layer Network) . 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 بمنظور 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 بمنظور 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 معمولا" 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، بمنظور 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 بمنظور 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 .

۲-۶ : نصب و راه اندازی شبکه :

امروزه برای ایجاد شبکه طرق مختلفی وجوددارد که کم هزینه ترین شبکه ها ،شبکه های بر پایه کابل می باشدکه در اینجا بحث اصلی طراحی و ایجاد اینگونه شبکه ها می باشد.

برای طراحی یک شبکه کامل چند پارامتر باید در نظر گرفته شود. اولین پارامتر تقسیم بندی شبکه براساس گستره جغرافیایی (Range) می باشدکه معمولاً شبکه های محلی یا LAN را درنظر گرفته ایم،دومین گزینه تقسیم بندی شبکه براساس گره (Node)می باشد که بطور معمول از شبکه های مبتنی بر سرور یاد می کنیم.در این حالت یک کامپیوتر به عنوان یک سرویس ددهنده عمل کرده وبه تنهایی به چندین کامپیوتر دیگر سرویس خواهد داد. پارامتر بعدی جهت تقسیم بندی شبکه نوع توپولوژی شبکه می باشدکه بطور متداول بهترین توپولوژی چه از لحاظ ترکیب و چه ازلحاظ امنیت توپولوژی Star می باشد. البته این توپولوژی هم دارای معایبی است از جمله حجم زیاد کابل کشی وهمچنین در صورت از کار افتادن قطعه مرکزی یا Hub کل شبکه از کارمی افتد.پارامترهایی نظیر پروتکل ،امنیت شبکه ، استاندارد و غیره هم مطرح میباشندکه از لحاظ نرم افزاری بیش تر قابل بحث می باشند.

حال جهت طراحی و پیاده سازی یک شبکه ، STAR LAN مبتنی به سرور چه باید کرد ؟ بهترین طراحی تقسیم یک شبکه به چندی زیر شبکه کوچک است . این عمل دارای مزایای فراوانی میباشد که از جمله :

- سیگنال الکتریکی هنگام عبور در طول کابل دچار تضعیف شده ، دامنه آن افت میکند ، که در صورت کوتاه بودن مسیر و طول کابل این مشکل زیاد تاثیر نمی گذارد .

۱- عیب یابی و اشکال زدایی در یک شبکه بمراتب خیلی راحتتر از یک شبکه بزرگ است .

۲- در صورت بروز مشکل در یک زیر شبکه فقط قسمت کوچکی از شبکه از کار می افتد و بقیه شبکه همچنان به کارخود ادامه میدهد.

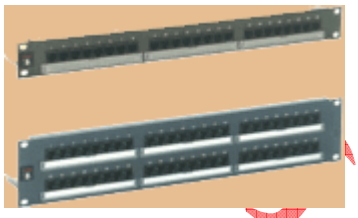
۳- هزینه های خرید وتهیه سخت افزار کاملا کاهش می یابد و با به اشتراک گذاردن تجهیزات نیاز تمام کاربران برطرف می شود.

چه نوع کابلی را باید انتخاب کنیم ؟

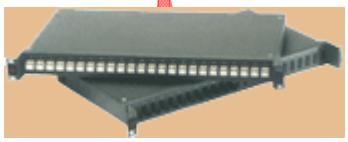
معمولا برای آنکه هزینه نصب و راه اندازی شبکه را کاهش دهیم از کابلهای UTP استفاده میکنیم ، پدیده ای بنام تداخل الکترومغناطیسی (EMI) باعث تضعیف سیگنالهای الکتریکی میشود . از طرفی تابیدگی کابل UTP مقدار EMI را کاهش میدهد که این تابیدگی در کابلهای CAT ۵e نسبت به CAT۵زیاد میباشد ، و در کابلهای CAT۶ باتوجه به تکنولوژی حاضر به اوج خود رسیده که علاوه بر تابیدگی زوج سیمها بدور هم ، چهار زوج دوباره به دوریکدیگر روی یک محوری از PVC تابیده شده اند . در نتیجه این گونه سیمها در شرایط مطلوب توانایی انتقال دیتاتا ۱۰۰۰ Mbpsرا دارند . البته نحوه کابل کشی ، نحوه اتصالات ، استفاده از انواع پریز های مرغوب و با کیفیت ، استفاده ازانواع

Patch Cordآماده با پلاستیک تزریقی بجای نوع مشابه دست ساز ،استفاده از Patch Panel های خاص و مرغوب و ... همگی در میزان سرعت انتقال دیتا تاثیربسزایی دارند.

آیا Hub بهتر است یا Hub – Switch و یا Switch ؟



در یک شبکه ، سیمهای کابل های UTP را نمی توان به یکدیگر لحیم کرد ، زیرا این عمل موجب ایجاد نویز و اعوجاج در سیگنالهای شبکه میشود . برای جلوگیری از بروز این مشکلات از دستگاه مرکزی بنام (Hub) در شبکه ها استفاده میشود . یک هاب به قطعات شبکه سازمان بخشیده و سیگنالهای دریافتی را به دیگر قسمت ها ارسال میکند .



هاب سوئیچ ها ، هاب هایی هستند که مستقیما در گاهها را به یکدیگر

سوئیچ می کنند و مانند هابهای دو سویه عمل میکنند یعنی اجازه ارتباط دو طرفه را می دهند ، بنابر این پهنای باند در دسترس به دو برابر فزایش می یابد . تنها تفاوت در این است که بین همه درگاهها کانال ۱۰ مگابیتی یا ۱۰۰ مگابیتی برقرار است .

امروزه سوئیچ ها در اغلب شبکه های LAN جایگزین هاب ها شده اند ، و عموما دو عمل اساسی را انجام میدهند:

۱- سوئیچ کردن قاب داده ها، فرآیند دریافت یک بسته دیتا در رسانه ورودی وانتقال آن به رسانه خروجی.

۲- نگهداری عملیات سوئیچینگ ، سوئیچ ها جدول های سوئیچینگ می سازد و از آن نگهداری می کنند.

مزایای سوئیچ ها :

۱- یک سوئیچ اترنت مزایای زیادی دارد ، از قبیل اجاره به تعدادی کاربر برای برقراری ارتباط موازی از طریق استفاده از مدارهای مجازی و قسمتهای اختصاصی شبکه در یک محیط عاری ازبرخوردیعنی از طریق پهنای باندبیشتر آزاد و هر کاربر پهنای باند مخصوص به خود دارد.

۲- مزیت دیگر آن این است که جایگزینی آن با هاب بسادگی انجام پذیر است ونیازی به تعویض سخت افزار و کابلهای موجود نمی باشد و بالأخره مدیر شبکه به سادگی میتواند آنرا مدیریت کند.

۳- سوئیچ ها درلایه پیوند داده ای (از لایه های شبکه) کار می کنند و همانند پلها اجازه اتصا ل Segmentهای LAN به یکدیگر برای تشکیل یک شبکه بزرگتر را مید هند.

۴- سوئیچ ها ترافیک را کاهش میدهدو در نتیجه نسبت به دیگر تجهیزات فعال شبکه از سرعت بالاتری برخوردار هستند و می توانند از کاربر های جدیدی همانند VLAN (LANمجازی) پشتیبانی

کنند .

۲-۷ : PDA :

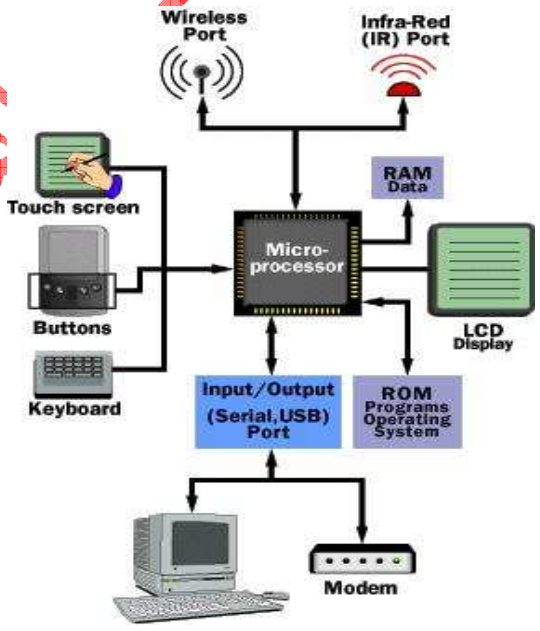
امروزه در اغلب کشورهای پیشرفته از notbook و یا organizer در موارد متعددی استفاده بعمل می آید. با استفاده از دستگاههای فوق هر شخص دارای دفترچه آدرس ، برنامه ریزی روزانه ، لیست کارهائی که می بایست انجام شود ، دفترچه یاداشت ، ماشین حساب ، لیست پروژه ها و سایر گزارشات متنوع و مورد نیاز خود بوده در صورت لزوم قادر به استفاده سریع از آنان خواهد بود. دستگاههای فوق دارای تمام امکانات لازم بمنظور برنامه ریزی و سازماندهی فعالیت های رایج زندگی می باشند. طی سالیان اخیر دستگاه جدیدی با قابلیت های بمراتب بیشتر عرضه شده است که با استقبال چشمگیر خریداران مواجه شده است . دستگاههای فوق PDA(Assistants Personal Digital) نامیده می شوند. PDA کامپیوترهای قدرتمندی بوده که براحتی در یک دست قرار می گیرند. عملکردPDA دربرخی موارد مشابه Organizer است ، با این تفاوت که با استفاده از PDA می توان نامه های الکترونیکی خود را دریافت و یا به موسیقی گوش داد. میزان فروش PDA از زمان عرضه تاکنون یک رکورد تاریخی را ثبت کرده است . تاکنون بیش از نه میلیون کامپیوتر دستی (PDA) فروخته شده است . اکثر PDA فروخته شده متعلق به شرکت Palm می باشند. شرکت های دیگر نیز محصولات خود را در این زمینه تولید و به بازار عرضه

نموده اند ، بنابراین با توجه به رقابت موجود می توان نمونه ای را تهیه نمود که دقیقا" منتاسب با خواسته های هر فرد باشد.

مبانی PDA :

PDA به دو گروه عمده: کامپیوترهای دستی ((Hand-held و کامپیوترهای Palm-Sized تقسیم می گردند. مهمترین تفاوت بین دو گروه فوق اندازه ، نوع نمایشگر و نحوه ورود اطلاعات است . کامپیوترهای دستی در مقایسه نسبت به کامپیوترهای Palm-Sized ، بزرگتر و سنگین تر می باشند. این نوع کامپیوترها دارای صفحات نمایشگر LCD بزرگتر ویک صفحه کلید کوچک بهمراه ترکیب تکنولوژی Touch-screen برای ورود اطلاعات می باشند. کامپیوترهای Palm-Sized سبک تر و کوچک تر می باشند. این نوع از کامپیوترها از صفحات نمایشگر LCD کوچک و تکنولوژی stylus/touch-screen و برنامه های تشخیص تایپ دستی برای ورود اطلاعات استفاده می نمایند.

شکل زیر عناصر تشکیل دهنده یک PDA را نشان می دهد.



شکل ۱۶-۲

صرفنظر از نوع PDA ، تمام آنها دارای پتانسیل های سخت افزاری مشابه ای می باشند:

- ریزپردازنده
- سیستم عامل
- حافظه
- باطری
- نمایشگرهای LCD
- دستگاه ورودی(دکمه هائی بهمراه نمایشگرهای touch-screen و یا صفحه کلید)
- پورت های ورودی و خروجی
- نرم افزارهای کامپیوترهای شخصی

ریزپردازنده :

دستگاههای PDA مشابه کامپیوترهای شخصی و یا Laptop از ریزپردازنده استفاده می نمایند. ریزپردازنده بمنزله مغز یک PDA بوده و تمام عملیات مربوطه را بر اساس دستورالعمل های برنامه ریزی شده انجام می دهند. برخلاف کامپیوترهای شخصی ، دستگاههای PDA از ریزپردازنده های کوچکتر و ارزانتر استفاده می نمایند. پردازنده های Motorola Dragonball و هیتاچی SH۷۷۰۹a نمونه هائی در این زمینه می باشند. با اینکه سرعت پردازنده های فوق در مقایسه با پردازنده های استفاده شده در کامپیوترهای شخصی بمراتب کمتر است (سرعت پردازنده های فوق بین ۱۶ تا ۷۵ مگاهرتز می باشد) ولی پردازنده استفاده شده در این نوع از کامپیوترها متناسب با وظایفی است که بر عهده آنان گذاشته شده است . ابعاد کوچک و قیمت پایین این نوع از کامپیوترها ، سرعت پایین (نسبت به کامپیوترهای شخصی) آنها را کم رنگ می نماید. شکل زیر یک نمونه از ریزپردازنده های Motorola Dragonball را نشان می دهد.

شکل ۱۷-۲

سیستم عامل :

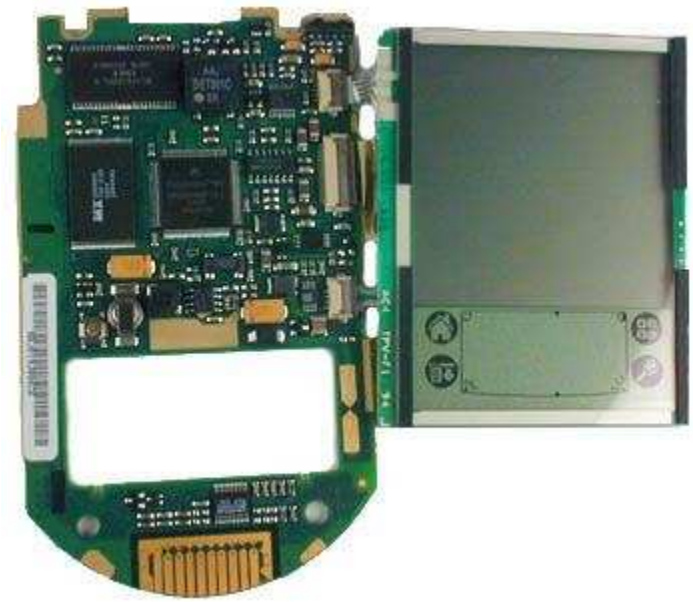
سیستم عامل شامل دستورات از قبل برنامه نویسی شده ای می باشد که به پردازنده عملیات مربوطه را دیکته خواهد کرد. سیستم های عامل استفاده شده در کامپیوترهای PDA به پیچیدگی سیستم های عامل استفاده شده در کامپیوترهای شخصی نمی باشند. این نوع از سیستم های عامل دارای مجموعه دستورات کمتری بوده که به حافظه کمتری نیاز خواهند داشت . مثلا" سیستمعامل Palm به ۱۰۰کیلو بایت حافظه بیشتر نیاز ندارد.(کمتر از یک درصد نسبت به حافظه مورد نیاز برای نصب ویندوز ۹۸ و یا MAC OS) . کامپیوترهای PDA عمدتا" از دو نوع سیستم عامل استفاده می نمایند : Palm OS(۳ COM یا PocketPC . سیستم عامل Palm os ، به حافظه کمتری نیاز داشته و دارای سرعت بیشتر می باشد. اغلب کاربران نیز از سادگی استفاده از سیستم عامل Palm ابراز رضایت می نمایند.سیستم عامل PocketPC نمایشگرهای رنگی، گرافیک، نسخه های خاصی از نرم افزارهای Word,Excel و سایر دستگاهها (نظیر Built-in MP۳ player,MPEG movie Player) را حمایت می نماید. سیستم عامل فوق با توجه به ماهیت خود به فضای بیشتری از حافظه نیاز نداشته و سرعت آن نسبت به Palm

Os کمتر است . با توجه به گسترش استفاده از این نوع کامپیوترها در سطح جهان ، شرکت های متعددی در حال پیاده سازی نرم افزارهای خاص برای استفاده تحت دو سیستم عامل فوق می باشند.

حافظه :

کامپیوترهای PDA دارای هارد دیسک نمی باشند. برنامه های مورد نظر (دفترچه تلفن ، ماشین حساب ، دفترچه یاداشت و سیستم عامل) در یک نوع حافظه ROM ذخیره می گردند. اطلاعات فوق زمانیکه کامپیوتر خاموش است ، همچنان در حافظه باقی خواهند ماند. داده ها و سایر برنامه هائی که توسط کاربران اضافه می گردد ، در حافظه RAM دستگاه ذخیره می گردند. رویکرد فوق نسبت به کامپیوترهای شخصی دارای چندین مزیت است .زمانیکه PDA روشن می گردد ، تمام برنامه ها بلا فاصله قابل استفاده بوده و نیازی به معطل شدن برای فعال شدن هر یک از برنامه ها نخواهد بود. زمانیکه محتویات یک فایل تغییر داده می شود ، اطلاعات جدیدد بصورت اتوماتیک ذخیره خواهند شد و نیازی به استفاده از دستور Save نخواهد بود. زمانیکه دستگاه خاموش می گردد ، اطلاعات همچنان در حافظه باقی خواهند ماند.(چون از باطری استفاده می گردد). تمام کامپیوترهای PDA از حافظه های Solid-state استفاده می نمایند. برخی از حافظه Static RAM و برخی دیگر از حافظه Flash استفاده می نمایند. برخی دیگر نیز از حافظه های قابل حمل (تعویض) استفاده می نمایند. حداقل حافظه کامپیوترهای PDA دو مگابایت است . برخی از مدل های پیشرفته PDA دارای حافظه ای بین ۵ تا ۳۲ مگابایت می باشند. سیستم عامل PocketPC نسبت به Palm OS فضای بیشتری از حافظه را اشغال خواهند کرد ، بنابراین کامپیوترهای PDA که از سیستم عامل PocketPC استفاده می نمایند ، بین ۱۶ تا ۳۲ مگابایت حافظه استفاده می گردد. در برخی از مدل های PDA امکان ارتقاء حافظه نیز وجود دارد.

شکل زیر نمای درون یک PDA را نشان می دهد. درقسمت میانی برد فوق ، پردازنده قرار گرفته و در سمت چپ و در بخش بالای ریزپردازنده ، تراشه های حافظه قرار گرفته اند.



شکل ۱۸-۲

باطری :

برق مورد نیاز کامپیوترهای PDA توسط باطری تامین می گردد. برخی از مدل های PDA از باطری الکالاین (AAA) استفاده می نمایند. برخی دیگر از مدل های PDA از باطری های با قالبیت شارژ مجدد(Lithium,nickel-cadmium,nickel-metal hybride) استفاده می نمایند عمر مفید باطری بستگی به PDA و نوع استفاده از آن دارد. موارد زیر باعث مصرف بالای باطری می گردد:

- سیستم عامل
- حافظه بیشتر
- نمایشگرهای LCD رنگی

- ضبط صوت
- Mp۳ Player

عمر یک باطری می تواند از دو ساعت تا دو ماه، باتوجه به نوع PDA و امکانات مربوطه باشد . اکثر کامپیوترهای PDA دارای سیستم مدیریت Power می باشند. سیستم فوق باعث افزایش عمر مفید یک باطری می گردد. در صورتیکه عمر باطری بگونه ای باشد که نتوان دستگاه را روشن نمود (پیشاپیش هشدار خواهد داد) ، به اندازه کافی برای نگهداری اطلاعات موجود در RAM فرصت خواهد بود. در صورتیکه عمر مفید باطری بطور کامل به اتمام رسیده باشد و یا آنها را از دستگاه خارج کرده باشید ، تقریبا" یک دقیقه فرصت خواهد بود تا باطری را تعویض نمود (ترانزیستور موجود در سیستم شارژ خود را ازدست نداده باشد) در صورت تخلیه شارژ ترانزیستور موجود در سیستم و عدم استفاده از زمان یک دقیقه ای بمنظور تعویض باطری ، اکثر دستگاههای PDA اطلاعات خود را از دست خواهند داد. با گرفتن Backup از اطلاعات موجود در PDA بر روی یک کامپیوتر شخصی و یا یک LapTop می توان اثرات جانبی را به حداقل مقدار خود رساند. دستگاههای PDA دارای آداپتورهای AC برای استفاده از برق شهری نیز می باشند.

نمایشگر LCD :

کامپیوترهای PDA دارای یک نوع خاص از صفحات نمایشگر LCD می باشند. برخلاف کامپیوترهای شخصی که نمایشگرهای LCD بعنوان دستگاههای خروجی مورد استفاده قرار می گیرند ، دستگاههای PDA از نمایشگرهای خود برای ورودی و خروجی استفاده می نمایند. نمایشگرهای LCD دستگاههای PDA بمراتب کوچکتر از نمایشگرهای laptop است . کامپیوترهای Hand-held (نوعی خاص از دستگاههای PDA) از صفحات نمایشگر بزرگتری نسبت به کامپیوترهای Palm-Sized استفاده می نمایند. نمایشگرهای PDA دارای ویژگی های زیر می باشند :

- LCD و یا Enhanced LCD و یا CSTN
- دارای وضوح تصویر ۱۶۰*۱۶۰ و ۳۲۰ * ۲۴۰ می باشند
- سیاه و سفید (۱۶ رنگ خاکستری) و یا رنگی (۶۵.۵۳۶ رنگ)
- ماتریس های Active و یا Passive (ماتریس های Active شفاف تر و خواندن اطلاعات آسان تر است)
- Reflective و یا Backlit . (نمایشگرهای Backlit برای استفاده در نور پایین مناسب می باشند)

دستگاه ورودی :

در کامپیوترهای PDA ، بمنظور ورود اطلاعات و دستورات از روش های متفاوتی استفاده می شود.کامپیوترهای Hand-held عموما" از یکدستگاه صفحه کلید خیلی کوچک و ظریف همراه با یک touch-screen استفاده می نمایند. کامپیوترهای palm-Sized از یک قلم فولادی و یک touch-screen همراه با یک برنامه تشخیص تایپ دستی استفاده می نمایند. هر یک از مدل های فوق دارای مجموعه ای از دکمه ها بمنظور فعال کردن نمایشگر و یا برنامه ها می باشند.

نمایشگر کامپییوترهای Palm-sized ، یک صفحه بسیار نازک چهار اینچی است که از آن هم بعنوان دستگاه ورودی و هم بعنوان دستگاه خروجی استفاده می گردد.کامپیوترهای فوق بمنظور نمایش اطلاعات از یک LCD استفاده می نمایند. در قسمت بالای LCD یک touch-screen وجود داشته که می توان با استفاده از یک مداد شبه فولادی و یا ورود مستقیم داده ، اطلاعاتی را وارد کرد. زمانیکه مداد فولادی با صفحه تماس برقرار می نماید ، روکش پلاستیکی موجود بر روی نمایشگر ، به سمت پایین حرکت تا با سطح شیشه ای تماس برقرار نماید. عملیات فوق باعث می گردد یک میدان ولتاژ ایجاد گردد ، میدان فوق توسط درایورtouch-screen ضبط می گردد. با ارسال یک جریان الکتریکی افقی و در ادامه عمودی ،

touch-screen مختصات X,Y مربوطه به نقطه مورد نظر را بدست می آورد. درایور در هر ثانیه هزاران مرتبه touch-scrren را پیمایش و اطلاعات مورد نظر را برای هر یک از برنامه هائی که به آنها نیاز دارند ، ارسال می دارند.

همانگونه که اشاره گردید یکی دیگر از روش های ورود اطلاعات در کامپیوترهای Palm-Sized ، استفاده از یک برنامه تشخیص تایپ دستی است . با استفاده از مداد فولادی بر روی نمایشگر کاراکترهائی رسم می گردد. نرم افزارهمراه PDA ، کاراکترهای رسم شده را به حروف و یا ارقام تبدیل می نماید. در دستگاههای Palm ، نرم افزاری که حروف را تشخیص می دهد Graffiti نامیده می شود. بمنظور کمک به تشخیص کاراکترها توسط برنامه فوق ، می بایست حروف در یک بخش صفحه و ارقام در بخش دیگر رسم گردند. هر کاراکتر می بایست با یک حرکت بدون توقف رسم گردد. بدین منظور می بایست از حروف " الفبائی مخصوص " استفاده کرد. مثلا" برای نوشتن حرف "A" می بایست "V" و یا برای حرف F"" از یک L وارونه استفاده گردد.

یکی از اشکالات نرم افزار تشخیص تایپ دستی ، نیاز به فراگیری روش های جدید برای نوشتن است . سرعت نوشتن با استفاده از روش فوق نسب به تایپ دستی کند تر است . در صورت تمایل می توان از یک صفحه کلید Onscreen استفاده و از مشکلات اشاره شده برحذر ماند. صفحه کلید فوق مشابه یک صفحه کلید معمولی است . تنها تفاوت موجود استفاده از مداد فولادی برای ضربه زدن و فشردن هر یک از کلیدهای مورد نظر بر روی صفحه کلید است . برخی از مدل های کامپیوترهای Palm دارای امکان جانبی صفحه کلید می باشند. استفاده از صفحه کلید فوق بمراتب راحتر از سایر موارد اشاره شده بوده خصوصا" در زمان ارسال E-mail است . اخیرا" برخی از مدل های PDA از تکنولوژی تشخیص صوت نیز استفاده می نمایند. در این مدل ها می توان با استفاده از میکروفن اطلاعات خود را بصورت صوتی وارد و توسط نرم افزار مربوطه عملیات تبدیل صوت به داده انجام خواهد شد.

دستگاههای ورودی و خروجی :

کامپیوترهای PDA بگونه ای طراحی شده اند که تحت هر شرایطی قادر به استفاده از کامپیوترهای شخصی و یا Laptop باشند. مثلا" می توان اطلاعاتی را از کامپیوتر شخصی خود به PDA منتقل و یا اطلاعات را از PDA به کامپیوتر منتقل نمود. بنابراین یک PDA می بایست قادر به ارتباط با یک کامپیوتر شخصی باشد. مبادله اطلاعاتی بین PDA و PC اصطلاحا" synchronization data نامیده می شود. ارتباطات فوق در کامپیوترهای PDA از طریق پورت USB انجام می گیرد. علاوه بر استفاده از کابل ، بمنظور تبادل اطلاعات ، برخی از دستگاههای PDA دارای یک پورت مادون قرمز بوده که از امواج نوری برای تبادل اطلاعات بین یک کامپیوتر شخصی و PDA استفاده می شود. برخی دیگر از مدل های PDA از روش های بدون کابل برای تبادل اطلاعات استفاده می نمایند. استفاده کنندگان PDA بمنظور دریافت و یا ارسال e-mail می بایست از یک ISP که امکان "بدون کابل " را نیز ارائه می دهد ، استفاده گردد. برخی دیگر از مدل های PDA دارای یک امکان جانبی بمنظور استفاده از مودم می باشند. امکان فوق بصورت جداگانه می بایست تهیه گردد.

نرم افزارهای کامپیوترهای شخصی و یا Laptop :

بمنظور ارسال اطلاعات از دستگاه PDA به کامپیوتر های شخصی و بالعکس ، می بایست از نرم افزارهای خاصی نظیر : HotSync برای کامپیوترهای PDA که از سیستم عامل Palm OS و یا ActiveSync برای کامپیوترهائی که از سیستم عامل PocketPc استفاده می نمایند ، استفاده گردد. نرم افزار فوق می بایست بر روی هارد دیسک کامپیوتر شخصی نصب تا امکان اتصال PDA به کامپیوتر شخصی توسط یکی از روش های : کابل ، اشعه مادون قرمز ، بدون کابل و یا مودم فراهم گردد. با توجه به گسترش دستگاه های PDA شرکت های متعددی در سطح جهان اقدام به طراحی و پیاده سازی نرم افزارهای مختص این نوع از سیستم ها نموده اند.

قابلیت های PDA :

دستگاههای PDA در ابتدا مشابه organizers رفتار می نمودند. آنها قادر به ذخیره آدرس ، شماره تلفن ، ثبت قرار ملاقات های روزمره و ... بودند. دستگاههای PDA در حال حاضر نیز عملیات فوق را انجام می دهند. پس از گذشت مدت زمانی کوتاه دستگاههای PDA متحول و پتانسیل های متعددی در آنها ایجاد گردید. امروزه با استفاده از دستگاههای PDA می توان اقدام به ارسال و یا دریافت E-mail و یا بازیابی اطلاعات مورد نیاز از اینترنت ، نواختن موزیک ، مشاهده فیلم و بازیهای ویدئویی نمود. برخی از قابلیت های PDA بشرح زیر می باشند:

- مدیریت اطلاعات شخصی (تمام مدل ها) .
- ذخیره اطلاعات مربوط به تماس با دیگران شامل : نام ، آدرس ، شماره تلفن ، آدرس E-mail
- ایجاد لیست فعالیت های روزمره
- یاداشت نویسی
- دفترچه یاداشت
- ثبت زمان وتاریخ قرار ملاقات ها
- یادآوری قرار ملاقات
- برنامه ریزی پروژه ها
- ماشین حساب
- ارسال و دریافت e-mail (برخی از مدل ها)
- استفاده از یک واژه پرداز (برخی از مدل ها)
- پخش فایل های موزیک mp۳ (برخی از مدل ها)
- پخش فایل های فیلم MPEG (برخی از مدل ها)
- دریافت اطلاعات دلخواه از اینترنت(برخی از مدل ها)

- بازیهای ویدئویی (برخی از مدل ها)
- ارتباط با سایر دستگاه ها نظیر دوربین های دیجیتال (برخی از مدل ها)

شکل ۱۹-۲

فصل سوم

نرم افزار شبکه

۱-۳: پروتکل های شبکه :

Packetها بلوک های اصلی انتقال اطلاعات در یک شبکه می باشند.همه اطلاعاتی که در یک شبکه منتقل می شوند در packetها قرار می گیرند و شامل اطلاعاتی درباره مبدا و مقصد اطلاعات می باشند.این packetها با بکارگیری استانداردها یا پروتکل ها ساخته شده اند.

می توان یک پروتکل را شبیه زبانی که کامپیوتر ما از آن جهت ارتباط با دیگر کامپیوترها روی یک شبکه استفاده می کند ،تصور کرد.درست همانطور که افراد جهان زبانهای مختلفی دارند،دنیای کامپیوترها نیز پروتکل های مختلفی دارد.اگر دو کامپیوتر پروتکل های متفاوتی برای ایجاد ارتباط با یکدیگر به کار برند هرگز نمی توانند با یکدیگر ارتباط برقرار کنند .این را شبیه ارتباط دو شخص که با زبان های مختلفی صحبت می کنند و سعی در ایجاد ارتباط با یکدیگر دارند تصور کنید،هیچگاه یک ارتباط واقعی اتفاق نمی افتد .اطلاعات فرستاده می شوند اما شخص یا کامپیوتر در یافت کننده نمی تواند آنها را بفهمد و قادر به فهم اطلاعات مربوط به دیگر زبان یا پروتکل نیست .

IPX/SPX:

این پروتکل بیشتر توسط Novell Netware(نسخه ۴.۱۱وقبل از آن)استفاده مشد ،چون نسخه های بعدی Netwareبطور پیش فرض TCP/IPرا بکار می برند.پروتکل IPX/SPXیک پروتکل Routableاست اما در اینترنت بکار نمی رود .این پروتکل سریعترین پروتکل Routableشبکه است .

TCP/IP:

امروزه بیشتر از این پروتکل استفاده می شود . پروتکل TCP/IPپروتکلی است که در اینترنت بکار می رود و معمولا با سیستم Unixرابطه دارد .

TCP/IPبرای استفاده DARPAوDODجهت ارتباط سیستم های آنها در کل کشور در سال

۱۹۷۰طراحی شد .این طراحی احتیاج به قابلیتی جهت غلبه بر حالات بی ثبات شبکه داشت .بنابر این طراحی TCP/IPشامل قابلیت مسیردهی مجدد Packetها بود.

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

- پروتکل 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.

یک مدیر شبکه خوب بایستی فهم واضحی از TCP/IPداشته باشد زیرا TCP/IPاینترنت و اینترنت Computingرا می گرداند.

:UDP

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 .

:Net BEUI

پروتکل انتقال است که معمولا در شبکه های کوچک وجود دارد .از این پروتکل در شبکه های بزرگ استفاده نمی شود و در آینده نیز کمتر بکار خواهد رفت زیرا Nonroutable است .

یک پروتکل Non routableپروتکلی است که قادر به حرکت در طول Routerنمی باشد . این بدان معناست که این پروتکل نمی تواند در یک شبکه WANاستفاده شود .

NetBEUIیک پروتکل بسیار سریع است .

مثال:

یک کمپانی قصد دسترسی به اینترنت را دارد اما پروتکلی که این شرکت در شبکه داخلی استفاده می کند روی شبکه اینترنت قابل استفاده نیست .این تنظیمات جهت امنیت منظور شده است بنابراین هیچ هکری نمی تواند به شبکه این کمپانی دسترسی پیدا کند و از هیچ جای WAN واز هیچ طریقی نمی توان به اطلاعات سرور دست یافت.چه پروتکلی می تواند از شبکه داخلی این کمپانی محافظت کند اما اجازه دسترسی به اینترنت را نیز به این شرکت بدهد؟

۱ - اولین چیزی که لازم است پروتکل TCP/IPاست .این پروتکل روی اینترنت بکار می رود .

۲ - دومین چیزی که لازم می باشد قابلیت دسترسی به اینترنت است که لازمه آن این است که یک دروازه جهت تغییر پروتکل داخلی

به TCP/IP در هنگام فرستادن داده ها به اینترنت و تغییر Packetهای TCP/IPاز اینترنت به پروتکل داخلی ،زمانی که داده ها از اینترنت فرستاده شده است ،داشته باشیم.

۳ - سناریو به یک WANاشاره دارد که بیشتر متناسب با اهمیت مسیریابها ست ،بنابراین یک پروتکل

مسیریاب Routableنیاز است بنابراین از NetBEUIنمی توانیم استفاده کنیم ،پس بایستی از IPX/SP در شبکه داخلی شرکت استفاده نماییم.

مدل OSI :

پروتکل OSI،گروهی از استانداردهای پروتکل هاست که به صورت استاندارد به یک ساختار منطقی برای عملیات شبکه تبدیل شده اند.این ساختار شامل ۷ لایه است .

ارتباطات شبکه در لایه Aplication شروع می شوند و به ترتیبف پله پله تا لایه فیزیکی پایین می آیند.اطلاعات پس از آن به کابل فرستاده می شوند تا کامپیوتری دیگر از شبکه که از لایه فیزیکی شروع به دریافت اطلاعات کرده آنها را دریافت نماید .در کامپیوتر گیرنده گام ها برعکس اجرا شده تا لایه Aplication ،جایی که پردازش توسط کامپیوتر دریافت کننده به اتمام رسیده پیش می رود.

پروتکل های مختلف در سطوح متفاوتی از مدل OSIعمل می کنند.در اینجا نگاهی می اندازیم به پروتکل های اصلی.

IPX :

IPX پروتکل جریان یافته بسیار سریع می باشد که اتصال گرا نمی باشد . ipxمی تواند در شبکه ای با ویندوز XPبکار رود.مهمترین مسئولیت ipxانتشار اطلاعات و داده هاست .IPXیک پروتکل Routableاست که در لایه شبکه مدل OSIعمل می کند.IPXتوانایی اجرا بر روی شبکه های Token RingوEthernetرا دارد.چندین سال IPXبطور پیش فرض NIc در شبکه های اترنت بکار می رفت.

:TCP/IP

TCP/IPپروتکل 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 میکند.

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

پروتکل TCP/IP در ابتدا برای استفاده در شبکه ARPAnet (نسخه قبلی اینترنت) طراحی گردید. وزارت دفاع امریکا با همکاری برخی از دانشگاهها اقدام به طراحی یک سیستم جهانی نمود که دارای قابلیت ها و ظرفیت های متعدد حتی در صورت بروز جنگ هسته ای باشد. پروتکل ارتباطی برای شبکه فوق ، TCP/IP در نظر گرفته شد..TCP/IPترکیبی از دو پروتکل متفاوت می باشد ،TCPوIP،هر دو در لایه های متفاوت مدل OSIبرای ساخت یک اساس و پا یه برای اجراهای دیگر و پرو تکل های لا یه های بالایی بکار می روند .

TCP/IP ترکیبی از دو پروتکل متفاوت است که در لایه های مختلف جاگذاری می شوند و کار می کنند .TCPدر لایه TransportوIPدر لایه Network.

TCPداده ها را به packetهای قابل مدیریت تقسیم می کند ;و IPاطلاعات را مسیردهی می کندو مبدا و مقصد آنها را مشخص می نماید .

TCP/IPروی شبکه های Token RingوEthernet عمل می کند.

: NFS

NFSپروتکلی است برای اشتراک فایلها تا کاربرانی که به شبکه متصل شدهاند بتوانند از منابع شبکه استفاده نمایند.این پروتکل توسط Sun Microsystems برای استفاده Solaris ساخته شد.بیشتر توسط Unix استفاده می شود.

NFS در لایهAplication مدل OSI کار می کند و عضوی از پرو تکل TCP/IP در نظر گرفته شده است.دلیل اصلی استفاده از این پروتکل ،دسترسی به منابعی که روی یک سرور Unix کار می کنند و یا اشتراک منابع با برخی اشخاصی که روی شبکهای با یک ایستگاه کاری Unix کار می کنند ، می باشد.

FTPوTFTP:

این دو پروتکل استانداردی از انتقال فایل بین دو سیستم می باشد . - پروتکل FTP (File Transfer Protocol) . از پروتکل فوق برای تکثیر فایل های موجود بر روی یک کامپیوتر و کامپیوتر دیگر استفاده می گردد. ویندوز دارای یک برنامه خط دستوری بوده که بعنوان سرویس گیرنده ایفای وظیفه کرده و امکان ارسال و یا دریافت فایل ها را از یک سرویس دهنده FTP فراهم می کند.FTP ،- connection oriented است یعنی این پرو تکل رسیدگی می کند که اطلاعات با موفقیت به سمت مقصد بروند.

TFTP عملکرد و هدفی مثل FTP دارد با این تفاوت که اتصال گرا نمی باشد و توجهی به این ندارد که Packet ها با موفقیت به مقصد برسند.به خاطر connection - oriented نبودن این پروتکل و به دلیل رسیدگی نکردن به درستی انتقال اطلاعات به مقصد ،احتیاج به Overhead کمتری جهت برقراری اتصال دارد ودر نتیجه سرعت TFTP از FTP بالاتر است.

SNMP:

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

:TelNet

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 .

:DECnet

پروتکلی است اختصاصی که توسط Digital Equipment Corporation برای استفاده در WAN ها توسعه یافته است .

می توانیم DECnet را در اترنت اجرا کنیم اما این به ندرت انجام می شود.این پروتکل Routable می باشد.

:SMTP

پروتکل SMTP(Protocol simple Mail Transfer) . از پروتکل فوق برای ارسال پیام الکترونیکی استفاده می گردد. پروتکلی است که ساختاری از پیغام های پستی اینترنت را معین می کند .این پروتکل بهترین ترکیب را برای انتقال استفاده می کند.

SMTP Session شامل اتصال SMTP ، فرستادن آدرس E-Mail مقصد ،فرستادن آدرس E-Mail مبدا وفرستادن عنوان و متن و بدنه پیغام E-Mail.

:DLC

این پروتکل زیاد معمول نیست .DLC، routableنمی باشدو بیشتر اوقات برای اتصال پرینترها به

سرورهایی که با ویندوزNTکار میکنند،بکار می رود.

HTTP :

پروتکل (Protocol HyperText Transfer(HTTP . 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.

:NNTP

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

:IP :۳-۲

۳-۲-۱: مدل آدرس دهی IP:

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

۳-۲-۲: نحوه اختصاص IP :

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

Subnetting :

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

۳-۲-۳: کالبد شکافی آدرس های IP :

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

- ۲۱۶.۲۷.۶۱.۱۳۷

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

- ۱۱۰۱۱۰۰۰.۰۰۰۱۱۰۱۱.۰۰۱۱۱۱۰۱.۱۰۰۰۱۰۰۱

همانگونه که مشاهده می گردد ، هر IP از ۳۲ بیت تشکیل می گردد. بدین ترتیب می توان حداکثر ۴.۲۹۴.۹۶۷.۲۹۶ آدرس منحصر بفرد را استفاده کرد($۲^{۳۲}$) . 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 دیگر بمنظور مشخص نمودن هر یک از کامپیوترهای میزبان استفاده می گردد. بدین ترتیب مجموع شبکه های کلاس A ، معادل ۱۲۶ و هر یک از شبکه های فوق می توانند ۱۶.۷۷۷.۲۱۴ کامپیوتر میزبان داشته باشند. (عدد فوق از طریق حاصل ۲ - $۲^{۲۴}$ 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
۲۴.۵۳.۱۰۷	۱۱۵.

- LoopBack . آدرس ۱۲۷.۰.۰.۱ IP برای LoopBack در نظر گرفته شده است . کامپیوتر میزبان از آدرس فوق برای ارسال یک پیام برای خود استفاده می کند.(فرستنده و گیرنده پیام یک کامپیوتر می باشد) آدرس فوق اغلب برای تست و اشکال زدائی استفاده می گردد.

- کلاس B . کلاس فوق برای شبکه های متوسط در نظر گرفته می شود.(مثلا" یک دانشگاه بزرگ) آدرس هائی که اولین octet آنها ۱۲۸ تا ۱۹۱ باشد ، کلاس B می باشند. در کلاس فوق از دومین octet هم برای مشخص کردن شبکه استفاده می گردد. از دو octet دیگر برای مشخص نمودن هر یک از کامپیوترهای میزبان در شبکه استفاده می گردد بدین ترتیب ۱۶.۳۸۴ ($۲^{۱۴}$) شبکه از نوع کلاس B وجود دارد. تعداد کامپیوترهای میزبان در این نوع شبکه ها(هر شبکه) معادل ۶۵.۵۳۴ (۲ - $۲^{۱۶}$) است .

بنابراین تعداد تمام کامپیوترهای میزبان در شبکه های کلاس B معادل ۱.۰۷۳.۷۴۱.۸۲۴ (۲۳۰) است در شبکه های کلاس B ، اولین و دومین بیت در اولین octet به ترتیب مقدار یک و صفر را دارا می باشند.

Host (Node)	NET
۵۳.۱۰۷	۱۴۵.۲۴.

- کلاس C . کلاس فوق برای شبکه های کوچک تا متوسط در نظر گرفته می شود.آدرس هائی که اولین octet آنها ۱۹۲ تا ۲۲۳ باشد ، کلاس C می باشند. در کلاس فوق از دومین و سومین octet هم برای مشخص کردن شبکه استفاده می گردد. از آخرین octet برای مشخص نمودن هر یک از کامپیوترهای میزبان در شبکه استفاده می گردد . بدین ترتیب ۲.۰۹۷.۱۵۲ (۲ ۲۱) شبکه کلاس C وجود دارد.تعداد کامپیوترهای میزبان در این نوع شبکه ها(هر شبکه) معادل ۲۵۴ (۲ - ۲ ۸) است . بنابراین تعداد تمام کامپیوترهای میزبان در شبکه های کلاس C معادل ۵۳۶.۸۷۰.۹۱۲ (۲۲۹) است . در شبکه های کلاس C ، اولین ، دومین و سومین بیت در اولین octet به ترتیب مقدار یک ، یک و صفر را دارا می باشند.

Host(Node)	NET
۱۰۷	۱۹۵.۲۴.۵۳.

- کلاس D . از کلاس فوق برای multicasts استفاده می شود. در چنین حالتی یک گره (میزبان) بسته اطلاعاتی خود را برای یک گروه خاص ارسال می دارد. تمام دستگاه های موجود در گروه ، بسته اطلاعاتی ارسال شده را دریافت خواهند کرد. (مثلا" یک روتر سیسکو آخرین وضعیت بهنگام شده خود را برای سایر روترهای سیسکو ارسال می دارد) کلاس فوق نسبت به سه کلاس قبلی دارای ساختاری کاملا" متفاوت است. اولین ، دومین ، سومین و چهارمین بیت به ترتیب دارای مقادیر یک ، یک ، یک و صفر می باشند.۲۸ بیت باقیمانده بمنظور مشخص نمودن گروههائی از کامپیوتر بوده که پیام Multicast برای آنان در نظر گرفته می شود. کلاس فوق قادر به آدرسی دهی ۲۶۸.۴۳۵.۴۵۶ (۲۲۶) کامپیوتر است

Host(Node)	NET
۲۴.۵۳.۱۰۷	۲۲۴.

- کلاس E . از کلاس فوق برای موارد تجربی استفاده می شود. کلاس فوق نسبت به سه کلاس اولیه دارای ساختاری متفاوت است . اولین ، دومین ، سومین و چهارمین بیت به ترتیب دارای مقادیر یک ، یک ، یک و یک می باشند.۲۸ بیت باقیمانده بمنظور مشخص نمودن گروههائی از کامپیوتر بوده که پیام Multicast برای آنان در نظر گرفته می شود. کلاس فوق قادر به آدرسی دهی ۲۶۸.۴۳۵.۴۵۶ (۲۲۶) کامپیوتر است .

Host(Node)	NET
۲۴.۵۳.۱۰۷	۲۴۰.

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

- ۲۵۵.۲۵۵.۲۵۵.۲۵۵.

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

- x.x.x.۱۰
- x.x - ۱۷۲.۳۱.x.x.۱۷۲.۱۶
- x.x.۱۹۲.۱۶۸

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

:

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

DNS
FlatNetBios NameSpace
اینترفیس های NetBios وWinSock
موارد اختلاف بین NetBios و WinSock
DNS Name Space
مشخصات دامنه و اسم Host
معرفی FQDN
طراحی نام حوزه برای یک سازمان
استفاده از نام یکسان دامنه برای منابع اینترنت و اینترانت
پیاده سازی نام یکسان برای منابع داخلی و خارجی

استفاده از اسامی متفاوت برای دامنه های اینترنت واینترانت

Authority Zones of

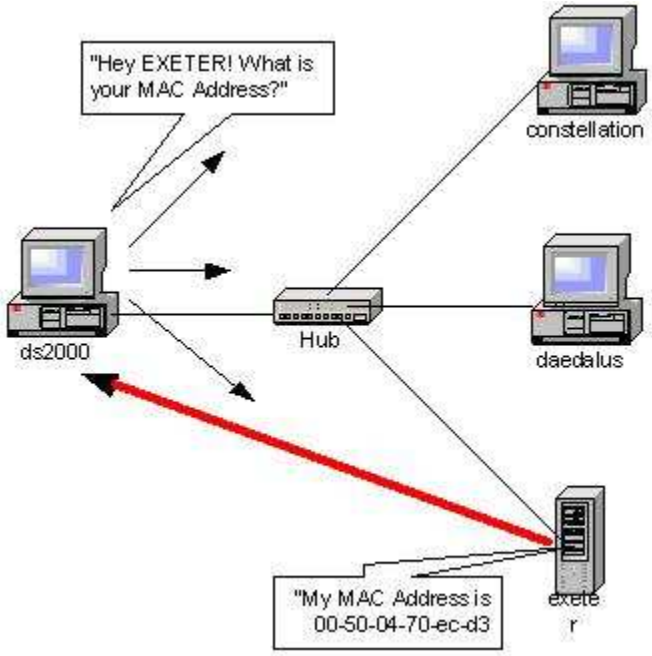
Lookup Zone Forward
تفاوت بین Domain و Zone
Reverse Lookup Zones

۳-۳: 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. بمنظور 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 شیکه 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 بمنظور 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 ds۲۰۰۰ 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 ds۲۰۰۰ ارسال می نماید.



شکل ۱-۳

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 Based Broadcast 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 برNetBIOS(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 صورتیکه 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" در شبکه 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

بمنظور 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 صورتیکه 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 صورتیکه 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 صورتیکه 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 .

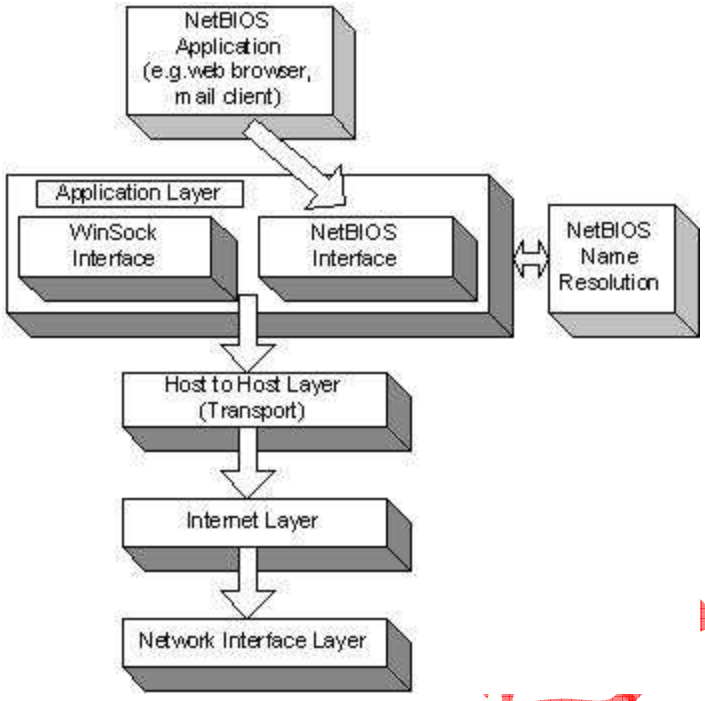
برنامه های با قابلیت اجراء بر روی شبکه هائی با سیستم های عامل مایکروسافت، با استفاده از دو روش متفاوت با پروتکل TCP/IP مرتبط می گردنند.

- **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 بمنظور ایجاد یک session انجام خواهند داد. در حالیکه پروتکل های (IP,TCP(TCP/IP) هیچگونه آگاهی از اسامی کامپیوترهای NetBIOS نداشته و در تمامی موارد مراقبت های لازم را انجام نخواهند داد.

بمنظور 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.



شکل ۲-۳

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 صورتیکه 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 Name Host 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.

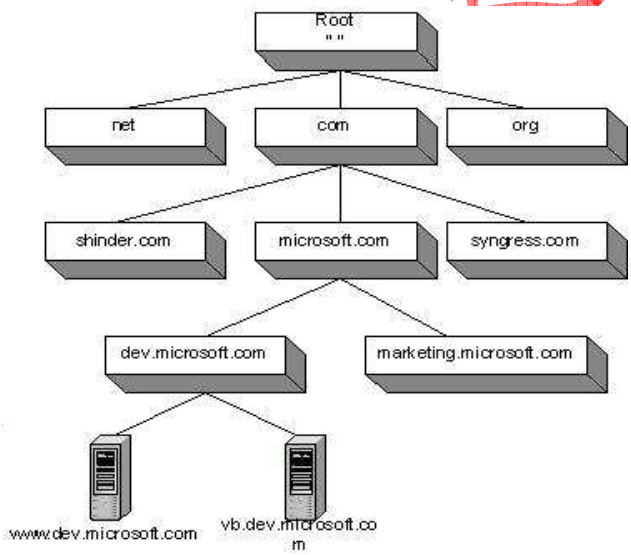
موارد اختلاف بین NetBIOS و WinSock:

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 .edu , .org , .net , Com 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. مثلا" 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.



شکل ۳-۳

در هر سطح از ساختار سلسله مراتبی فوق می بایست اسامی با یکدیگر متفاوت باشد. مثلا" 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 بخش هائی از سیستم DNS می باشند که می بایست

بصورت مرکزی مدیریت و کنترل گردنند. بمنظور 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. بمنظور 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 صورتیکه 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-۸ 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؟

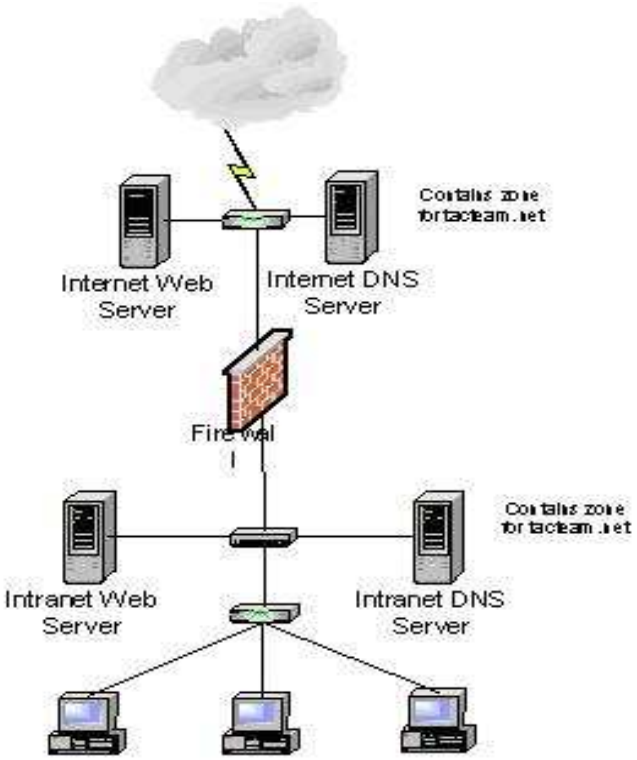
استفاده از نام یکسان دامنه برای منابع اینترنت و اینترانت:

استفاده از اسامی یکسان برای نامگذاری دامنه بمنظور 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. بمنظور 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 بمنظور دستیابی به اطلاعات اختصاصی و سایر اطلاعات داخلی سازمان استفاده می نمایند.در این مدل دارای سرویس دهندگانی خواهیم بود که بمنظور 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.



شکل ۴-۳

استفاده از اسامی متفاوت برای دامنه ها ی اینترنت و اینترانت:

در صورتیکه 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.

:Authority Zones of DNS

DNS دارای ساختاری است که از آن برای گروه بندی و دنبال نمودن ماشین مربوطه براساس نام host در شبکه استفاده خواهد شد. بمنظور 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%\system۳۲\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 .

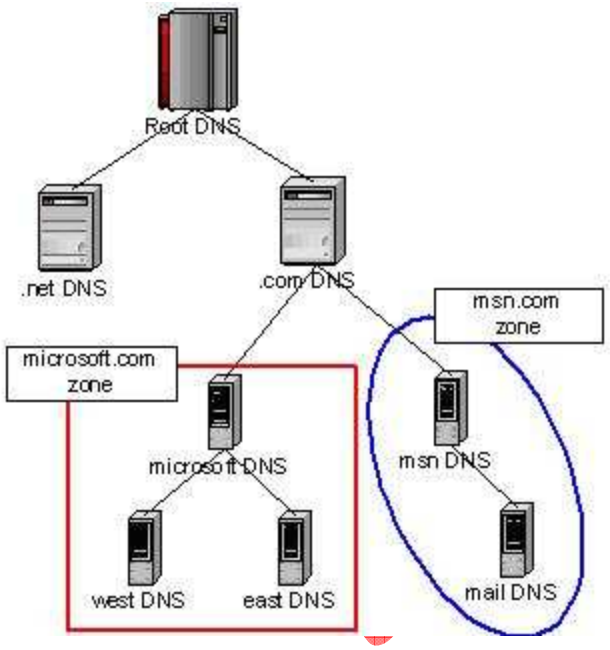
:Forward Lookup Zone

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 Resource Record " 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. (West.microsoft.com ,

East.microsoft.com). مایکروسافت دارای دامنه اختصاصی msn.com بوده که خود شامل دارای یک زیردامنه با نام mail.microsoft.com است .

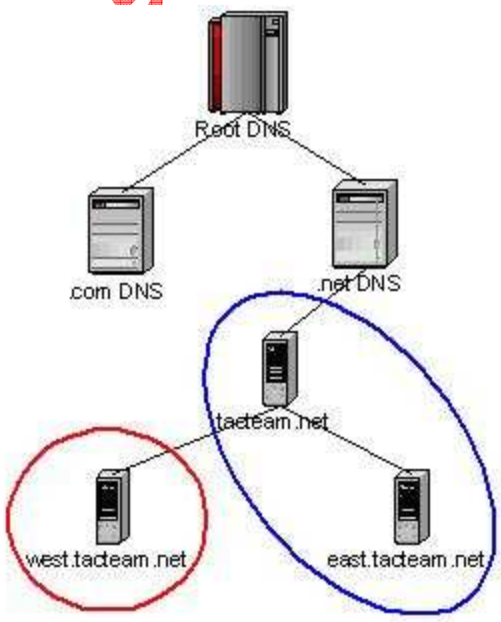


شکل ۵-۳

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 بمنظور 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 بمنظور 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 وضعینی 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.



شکل ۶-۳

Reverse Lookup Zones :

Zoneها ی از نوع Forward امکان ترجمه نام یک کامپیوتر به یک IP را فراهم می نمایند..یک Lookup Reverse 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 . بمنظور 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 صورتیکه 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. بمنظور حل مشکل فوق در رابطه با یافتن نام در صورتیکه 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 :

۱.۱۶۸.۱۹۲.in-addr.arpa.dns

مزایای DSL
اشکالات DSL
مبانی DSL
صوت و داده
تقسیم سیگنال
تجهیزات DSL
ترانسیور DSL
DSLAM
آینده DSL
HDSL
طرز کار خطوط DSL

۴-۳: 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.

DSL تکنولوژی است برای انتقال اطلاعات با پهنای باند بالا به خانه ها و businessهای کوچک از طریق خطوط تلفن مسی معمولی. XDSL بر انواع مختلف DSL دلالت میکند (مثل : ADSL ، HDSL ، RADSL و...).

بافرض اینکه خانه یا شرکت شما به اندازه کافی به شرکت تلفنی که به شما سرویس DSL ارائه میدهد نزدیک باشد، شما ممکن است قادر باشید که data را تا نرخ ۶.۱ Mbps دریافت کنید. همچنین قادر خواهید بود صدا، ویدئو وحتی effect های سه بعدی رابه راحتی وبه طور پیوسته انتقال دهید.

نصب DSL درسال ۱۹۹۸ آغاز شد وبه طورگستردهای دردهه آینده درآمریکا وکشورهای دیگرگسترش پیداخواهدکرد. شرکتهای Microsoft ، Intel ، Compaq باهمکاری شرکتهای تلفنی موفق شدهاند یک نسخه پیشرفته تر ازADSL رابوجود آورندکه از نظر نصب نیز بسیارآسان ترازنسخههای قبلی است این محصول، G.lite نامیده میشودکه به سرعت درحال گسترش میباشد.

به نظرمیرسدکه DSL دربسیاری ازمناطق جایگزین ISDN خواهدشد. ودررقابت با مودمهای کابلی (Cable Modem) برای استفاده از multimedia و D-۳ درخانه ها یا businessهای کوچک بسیارکارآمد میباشد.

مزایای DSL :

- در زمان اتصال به اینترنت ، امکان استفاده از خط تلفن برای تماس های مورد نظر همچنان وجود خواهد داشت .
- سرعت 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 (ایرادات) 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 آنچیزی 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 بمنظور انجام عملیات خاص)

بمنظور شناخت نحوه عملکرد DSL ، لازم است در ابتدا با یک خط تلفن معمولی آشنائی بیشتری پیدا گردد. 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 ۳۴۰۰ قابل انتقال است . محدوده فوق بسیار

ناچیز است . مثلا" در مقایسه با 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. در صورتیکه سرعت خط اینترنت به کاربر (دریافت اطلاعات) ، سه و یا چهار برابر سریعتر نیست.

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. بموزات افزایش طول خط ارتباطی ، کیفیت سیگنال افت و سرعت خط ارتباطی کاهش پیدا می

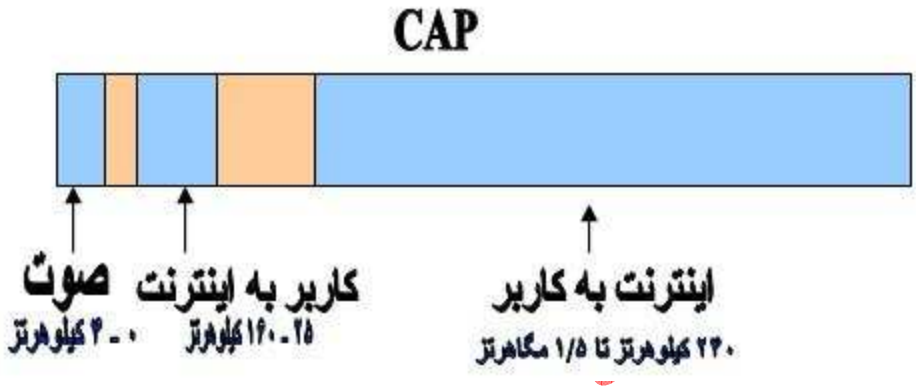
نماید. ADSL دارای محدودیت ۱۸.۰۰۰ فوت (۵.۴۶۰ متر) است . کاربرانی که در مجاورت و نزدیکی شرکت ارائه دهنده سرویس DSL قرار دارند، دارای کیفیت و سرعت مناسبی بوده و بموازات افزایش مسافت ، کاربران اینترنت از نظر کیفیت و سرعت دچار افت خواهند شد. تکنولوژی ADSL قادر به ارائه بالاترین سرعت در حالت " اینترنت به کاربر " (Downstream) تا ۸ مگابیت در ثانیه است .(در چنین حالتی حداکثر مسافت ۶.۰۰۰ فوت و یا ۱.۸۲۰ متر خواهد بود) . سرعت ارسال اطلاعات " از کاربر به اینترنت" (Upstream) دارای محدوده ۶۴۰ 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 ، ۶۴۰ 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، بمنظور 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 تلفن از فیبر نوری استفاده گردد ، 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 Multitone Discrete 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 Carrierless Amplitude/phase است (CAP) . استاندارد CAP ، سیگنال ها را به سه باند مجزا تقسیم می نماید : مکالمات تلفن دارای باند صفر تا ۴ کیلو هرتز، کانال دریافت اطلاعات از کاربر برای سرویس دهنده دارای

باندی بین ۲۵ تا ۱۶۰ کیلو هرتز (Upstream) و کانال ارسال اطلاعات از سرویس دهنده برای کاربر ، دارای محدوده ای که از۲۴۰ 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 ۱.۵ مگاهرتز تجاوز نخواهد کرد. سیستم CAP با استفاده از سه کانال فوق ، قادر به ارسال سیگنال های مربوطه خواهد بود.



شکل ۷-۳

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 ۲۴۷ کانال مجزا تقسیم می نماید.هر کانال دارای باند ۴ کیلو هرتز می باشند. (وضعیت فوق مشابه آن است که شرکت تلفن مربوطه ، خط مسی موجود را به ۲۴۷ خط ۴ کیلو هرتزی مجزا تقسیم و هر یک از خطوط فوق را به یک مودم متصل نموده است . استفاده همزمان از ۲۴۷ مودم که هر یک دارای باند ۴ 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 ۲۴۷ کانال

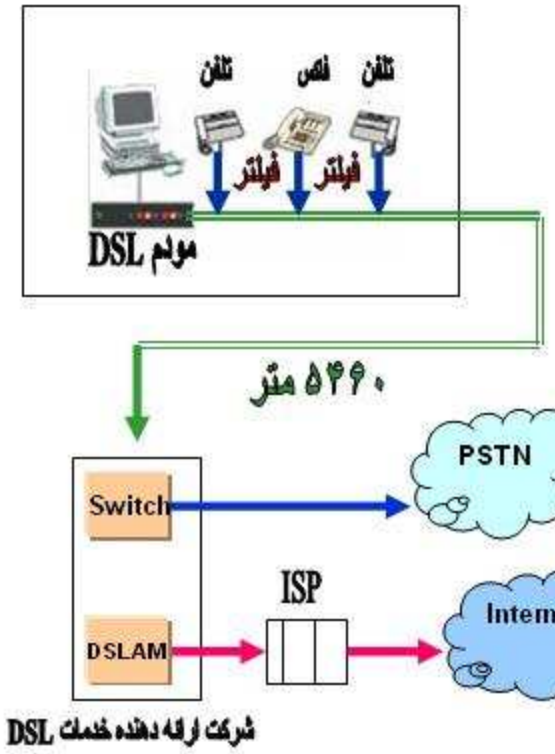
موجود ، پیاده سازی استاندارد DMT را نسبت به CAP بمراتب پیچیده تر نموده است . استاندارد DMT دارای انعطاف بمراتب بیشتری در رابطه با کیفیت خطوط و کانال ها ی مربوطه است .

شکل ۸-۳

استانداردهای CAP وDMT از دید کاربر دارای یک شباهت می باشند. در هر دو حالت از یک فیلتر بمنظور 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 ۴ 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 بمنظور دریافت اتصالات مشترکین استفاده می گردد. در ادامه به تشریح هر یک از دستگاههای فوق خواهیم پرداخت .



شکل ۹-۳

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 های کابلی تا سال ۱۹۹۹ به مرز ۱.۳۵۰.۰۰۰ کاربر رسیده

است . بر اساس پیش بینی بعمل آمده تا اواخر سال ۲۰۰۳ ، تعداد مشترکین مودم های کابلی 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 .

HDSL:

HDSL یکی ازقدیمیترین فرم های خطوط DSL میباشد که برای انتقالات دیجیتالی باند پهن (wideband) داخل سایت یک شرکت و یا بین شرکتهای تلفن و مشتری استفاده میشود. مهمترین خصوصیت HDSL متقارن بودن آن است (Symmetrical) . به این معنی که یک مقدار مساوی از پهنای باند دردوجهت (Receive , Send) دردسترس میباشد.ازآنجائیکه HDSL یکی از فرم های DSL است لازم است که ابتدا توضیحی درباره خطوط DSL داده شود:

طرز کار خطوط DSL:

سرویس تلفن سنتی ایجادشدتا اطلاعات Voice را بین کاربران منتقل کندو Signal هایی که برای این انتقال استفاده میشود analog نامیده میشوند. ازآنجاییکه درانتقال آنالوگ فقط قسمت کوچکی از مقدار اطلاعات موجود میتواند ازطریق خطوط مسی منتقل شود، ماکزیم مقدارdata که میتوانید از طریق مودم های معمولی دریافت کنید حدوداً ۵۶kbps میباشد. توانایی کامپیوترشمادردریافت اطلاعات محدود میشودبه این دلیل که: شرکت تلفنی اطلاعات دریافت شده به صورت دیجیتالی رابه فرم آنالوگ تبدیل میکندو روی خطوط تلفن شما میفرستد ومودم شما مجبور است دوباره آن رابه فرم دیجیتال تبدیل کند. به عبارت دیگر انتقال آنالوگ بین خانه یاشرکت تلفن یک پهنای باند خیلی باریک است.

درتکنولوژی DSL فرض براین است که نیازی نیست اطلاعات digital به analog تبدیل شودواطلاعات digitalبه طورمستقیم به کامپیوترشمامنتقل میشودواین به شرکت تلفن اجازه میدهدکه ازپهنای باندوسیعتری برای انتقال استفاده کند.

تکنولوژی DSL به شمااجازه میدهد که signal مجزاشودبطوریکه قسمتی از پهنای باند برای انتقال signalهای آنالوگ استفاده میشوددرنتیجه شمامیتوانیدهم ازکامپیوترهم از تلفن روی یک خط وبه طورهمزمان استفاده کنید.

اغلب تکنولوژیهای DSL نیازدارندکه یک جداکننده (Signal Splitter) درخانه یا محل شرکت شمانصب شود. البته میتوان عمل Splitting را از اداره مرکزی تلفن نیزانجام داد(Remote) این تکنولوژی تحت عنوان Splitterless DSL شناخته میشود.

HDSL قدیمیترین نسخه DSL است ومهمترین مزیت آن Symmetrical بودن آن است. علاوه براین HDSL قادر است روی یک کابل Twisted-pair به اندازه یک خط (T۱ تا ۱.۵۴۴ Mbps)درامریکای شمالی یا یک خط E۱ (تا ۲.۰۴۸ Mbps) دراروپا انتقال انجام دهد.

۵-۳: مد انتقال غیرهمزمان: ATM -Asynchronous Transfer Mode

ATM تکنولوژی برای انتقال داده های است که قابلیت متحول کردن روش ساخت شبکه های کامپیوتری را دارا است. این تکنولوژی که هم برای شبکه های LAN وهم برای شبکه های WAN ارزشمند است. سرعتهای بالایی برای انتقال دادهها فراهم کرده و انواع بسیار زیادی از ترافیکها، ازجمله صدا، داده ها، فکس، ویدیو، صدا باکیفیت CDو تصویر سازی را پشتیبانی میکند.

محصولات ATM عبارتند از:

- مسیریابهای ATM و سوئیچهای ATM که برای ساختن شبکه های عمومی سازمانی به خدمات ATM حامل متصل میشوند.
- دستگاههای ATM برای ساختن شبکه های Back bone خصوصی داخلی که تمامی شبکه های محلی (LAN های) سازمانها رابه یکدیگر متصل میکند.
- آداپتورهای ATM و سوئیچهای گروه کاری برای انتقال و استفاده از اتصالات ATM درکامپیوترهای شخصی ATM از مزیت انتقال بالای کابلهای فیبر نوری بهره میگیرد.
- ATM این قابلیت را دارد که به عنوان روش استاندارد انتقال دادهها جایگزین بسیاری از روشهای ارتباطاتی و صوتی امروز شود.

جنبه های تکنیکی ATM :

ATM تکنولوژی call relay باند گسترده برای انتقال صدا ، تصویر ودیتاست.(از طریق شبکه های WAN یا LAN).

دادهها درسلولهایی قرارمیگیرند که فریمهایی بااندازه ثابت بوده وبسته های دادهای قطعه بندی شده را حمل میکنند .

سلولها کوچک هستند و انتقال آنها از طریق سوئیچهای شبکه آسان است. بسته هایی که طول متغیر دارند، میتوانند برای مدت زمان نسبتا طولانی، سوئیچ رابه خود اختصاص دهند وچون اندازه فریمها متغیر است، جریان ترافیک غیرقابل پیشبینی است. این کار درمواقعی که بخواهید توان عملیاتی دادهها راتضمین کنید، مشکل ساز میشود مانند زمانی که بخواهید تصویر زنده را ارسال کنید.این تکنولوژِی، برای حل این مشکل فریمهای مختلف ا لطول را مجاز ندانسته و تنها با سلولهایی که طول ثابت دارند کار میکند.

لن های سنتی، همچون اینترنت، تو کن رینگ، از رسانه مشترکی که در آن در هرزمان تنها یک گروه قادر به انتقال داده هاست، استفاده میکنند. از طرف دیگر اتصالات چند به چند ارائه داده و گرهها میتوانند به

طور همزمان انتقال انجام دهند ، اطلاعات بسیاری از گرهها به صورت جریانی از سلولها تسهیم سازی میشود. در این سیستم، سوئیچ ای تی ام ممکن است متعلق به ارائه کننده سرویس عمومی یا بخشی از شبکه داخلی یک سازمان باشد.

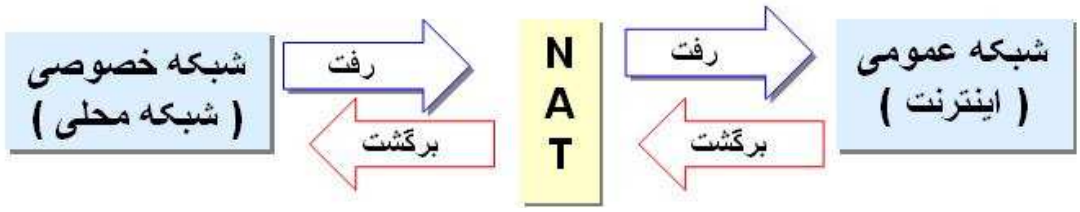
۳-۶: NAT:

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 (NAT) دارد؟ هر کامپیوتر بمنظور 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 ش بکه 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 ۴.۲۹۴.۹۷۶.۲۹۶ ($۲^{۳۲}$) 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 بعنوان یک آژانس بین اینترنت (شبکه عمومی) و یک شبکه محلی (شبکه خصوصی) رفتار نماید. این بدان معنی است که صرفا" یک IP منحصر بفرد بمنظور نمایش

مجموعه ای از کامپیوترها(یک گروه) مورد نیاز خواهد بود.



شکل ۱۰-۳

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

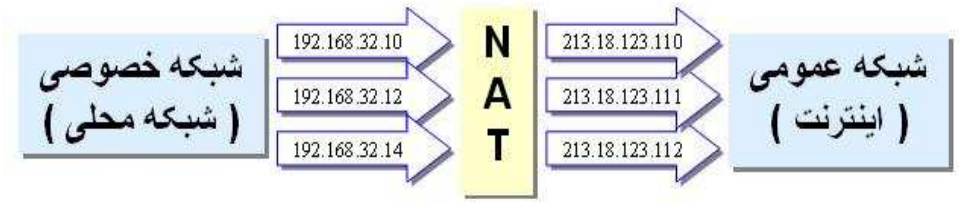
قابلیت های NAT:

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 بمنظور 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 .

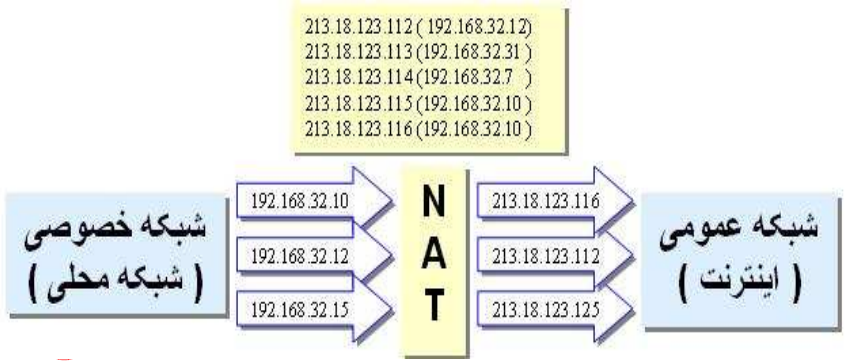
- NAT ایستا . عملیات مربوط به ترجمه یک آدرس IP غیر ریجستر شده (ثبت شده) به یک آدرس

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 ۱۹۲.۱۶۸.۳۲.۱۰ به IP ۲۱۳.۱۸.۱۲۳.۱۱۰ ترجمه خواهد شد.



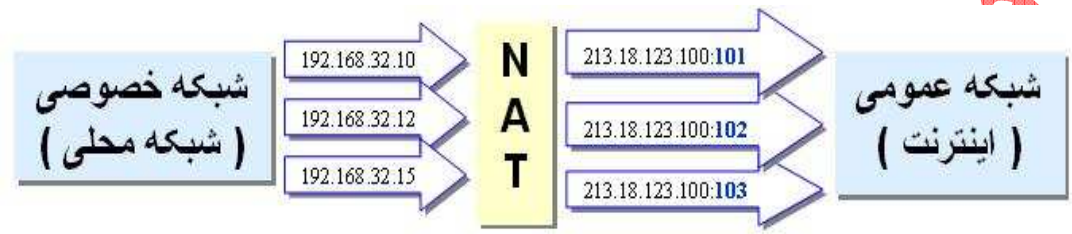
شکل ۱۱-۳

- 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.



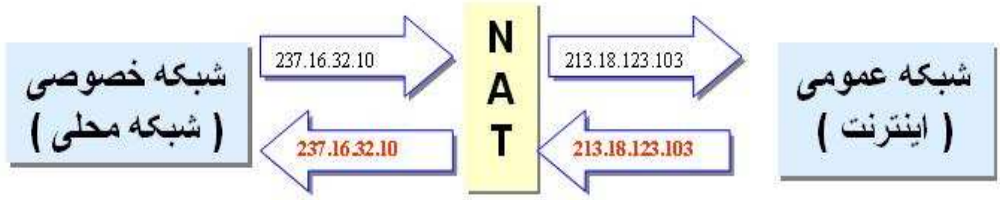
OverLoading –

. 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.



شکل ۱۳-۳

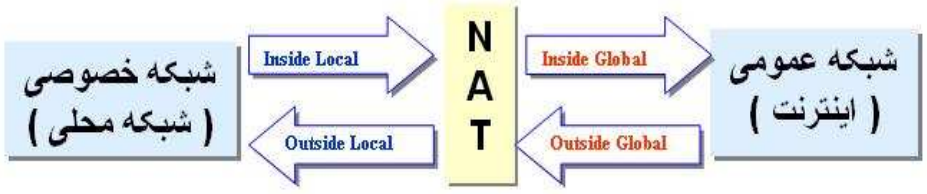
- Overlapping . در روش فوق شبکه خصوصی از مجموعه ای IP ریجستر شده استفاده می کند که توسط شبکه دیگر استفاده می گردند. NAT می بایست آدرس های فوق را به آدرس های IP ریجستر شده منحصربفرد ترجمه نماید. NAT همواره آدرس های یک شبکه خصوصی را به آدرس های ریجستر شده منحصر بفرد ترجمه می نماید. NAT همچنین آدرس های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



شکل ۱۴-۳

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 و بنابراین 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 بمنظور 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 - 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 غیرریجستر 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 address) . آدرس های Outside local بمنظور ترجمه به آدرس های منحصربفرد IP استفاده می شوند.آدرس های منحصر بفرد فوق، outside global نامیده شده و اختصاص به دستگاههای موجود بر روی شبکه عمومی (اینترنت) دارند.



شکل ۱۵-۳

- 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 صورتیکه 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 صورتیکه 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.

روش Overloading از یک ویژگی خاص پروتکل TCP/IP استفاده می نماید. ویژگی فوق این امکان را فراهم می آورد که یک کامپیوتر قادر به پشتیبانی از چندین اتصال همزمان با یک و یا چندین کامپیوتر با استفاده از پورت های متفاوت TCP و یا UDP باشد.. یک بسته اطلاعاتی IP دارای یک هدر(Header) با اطلاعات زیر است :

آدرس مبداء : آدرس کامپیوتر ارسال کننده اطلاعات است .

پورت مبداء. شماره پورت TCP و یا UDP بوده که توسط کامپیوتر مبداء به بسته اطلاعاتی نسبت داده شده است .

آدرس مقصد : آدرس کامپیوتر دریافت کننده اطلاعات است .

پورت مقصد. شماره پورتTCP و یا UDP بوده که کامپیوتر ارسال کننده برای باز نمودن بسته اطلاعاتی برای گیرنده مشخص کرده است .

آدرس ها ، کامپیوترهای مبداء و مقصد را مشخص کرده ، در حالیکه شماره پورت این اطمینان را بوجود خواهد آورد که ارتباط بین دو کامپیوتر دارای یک مشخصه منحصر بفرد است . هر شماره پورت از شانزده بیت استفاده می نماید .

NAT پویا و Overloading :

نحوه کار NAT پویا بصورت زیر است :

- یک شبکه داخلی (حوزه محلی) با استفاده از مجموعه ای از آدرس های IP که توسط Internet (IANA Authority) Assigned Numbers به شرکت و یا موسسه ای اختصاص داده نمی شوند پیکربندی می

گردد. (سازمان فوق مسئول اختصاص آدرس های IP در سطح جهان می باشد) آدرس های فوق بدلیل اینکه منحصربفرد می باشند، غیر قابل روتینگ نامیده می شوند.

- موسسه مربوطه یک روتر با استفاده از قابلیت های NAT را پیکربندی می نماید. روتر دارای یک محدوده از آدرس های IP منحصر بفرد بوده که توسط IANA د ر اختیار موسسه و یا شرکت مربوطه گذاشته شده است .

- یک کامپیوتر موجود بر روی حوزه محلی سعی درایجاد ارتباط با کامپیوتری خارج از شبکه (مثلا" یک سرویس دهنده وب) را دارد.

- روتر بسته اطلاعاتی را از کامپیوتر موجود در حوزه محلی دریافت می نماید.

- روتر آدرس IP غیرقابل روت را در جدول ترجمه آدرس ها ذخیره می نماید. روتر آدرس IP غیر قابل روت را با یک آدرس از مجموعه آدرس های منحصر بفرد جایگزین می نماید. بدین ترتیب جدول ترجمه، دارای یک رابطه (معادله) بین آدرس IP غیرقابل روت با یک آدرس IP منحصر بفرد خواهد بود.

- زمانیکه یک بسته اطلاعاتی از کامپیوتر مقصد مراجعت می نماید، روتر آدرس مقصد بسته اطلاعاتی را بررسی خواهد کرد.بدین منظور روتر در جدول آدرسهای ترجمه شده جستجو تا از کامپیوتر موجود در حوزه محلی که بسته اطلاعاتی به آن تعلق دارد، آگاهی پیدا نماید.روتر آدرس مقصد بسته اطلاعاتی را تغییر (از مقادیر ذخیره شده قبلی استفاده می کند) و آن را برای کامپیوتر مورد نظر ارسال خواهد کرد. در صورتیکه نتیجه جستجو در جدول، موفقیت آمیز نباشد، بسته اطلاعاتی دور انداخته خواهد شد.

- کامپیوتر موجود در حوزه ، بسته اطلاعاتی را دریافت می کند. فرآیند فوق مادامیکه کامپیوتر با سیستم خارج از شبکه ارتباط دارد، تکرار خواهد شد.

نحوه کار Overloading پویا بصورت زیر است :

- یک شبکه داخلی (حوزه محلی) با استفاده از مجموعه ای از آدرس های IP که توسط IANA (Internet Assigned Numbers Authority) به شرکت و یا موسسه ای اختصاص داده نمی شوند پیکربندی می گردد. آدرس های فوق بدلیل اینکه منحصربفرد می باشند غیر قابل روتینگ نامیده می شوند.

- موسسه مربوطه یک روتر را با استفاده از قابلیت های NAT ، پیکربندی می نماید. روتر دارای یک محدوده از آدرس های IP منحصر بفرد بوده که توسط IANA د ر اختیار موسسه و یا شرکت مربوطه گذاشته شده است .

- یک کامپیوتر موجود بر روی حوزه داخلی ، سعی درایجاد ارتباط با کامپیوتری خارج از شبکه(مثلا" یک سرویس دهنده وب) را دارد.

- روتر بسته اطلاعاتی را از کامپیوتر موجود در حوزه داخلی دریافت می نماید.

- روتر آدرس IP غیرقابل روت و شماره پورت را در جدول ترجمه آدرس ها ذخیره می نماید. روتر آدرس IP غیر قابل روت را با یک آدرس منحصر بفرد جایگزین می نماید. روتر شماره پورت کامپیوتر ارسال کننده را با شماره پورت اختصاصی خود جایگزین و آن را در محلی ذخیره تا با آدرس کامپیوتر ارسال کننده اطلاعات ، مطابقت نماید.

- زمانیکه یک بسته اطلاعاتی از کامپیوتر مقصد مراجعت می نماید ، روتر پورت مقصد بسته اطلاعاتی را بررسی خواهد کرد.بدین منظور روتر در جدول آدرس های ترجمه شده جستجو تا از کامپیوتر موجود در حوزه داخلی که بسته اطلاعاتی به آن تعلق دارد آگاهی پیدا نماید.روتر آدرس مقصد بسته اطلاعاتی و شماره پورت را تغییر (از مقادیر ذخیره شده قبلی استفاده می کند) و آن را برای کامپیوتر مورد نظر ارسال خواهد کرد. در صورتیکه نتیجه جستجو در جدول ، موفقیت آمیز نباشد بسته اطلاعاتی دور انداخته خواهد شد.

- کامپیوتر موجود در حوزه داخلی ، بسته اطلاعاتی را دریافت می کند. فرآیند فوق مادامیکه کامپیوتر با سیستم خارج از شبکه ارتباط دارد، تکرار خواهد شد.

- با توجه به اینکه NAT آدرس کامپیوتر مبداء و پورت مربوطه آن را در جدول ترجمه آدرس ها ذخیره شده دارد، مادامیکه ارتباط فوق برقرار باشد از شماره پورت ذخیره شده (اختصاص داده شده به بسته اطلاعاتی ارسالی) استفاده خواهد کرد. روتر دارای یک Timer بوده وهر بار که یک آدرس از طریق آن استفاده می گردد reset می گردد.در صورتیکه در مدت زمان مربوطه (Timer صفر گردد) به اطلاعات ذخیره شده در NAT مراجعه ای نشود، اطلاعات فوق (یک سطر از اطلاعات) از داخل جدول حذف خواهند شد.

در صورتیکه برخی ازکامپیوترهای موجود در شبکه خصوصی از آدرس های IP اختصاصی خود استفاده می نمایند ، می توان یک لیست دستیابی از آدرس های IP را ایجاد تا به روتر اعلام نماید که کدامیک از کامپیوترهای موجود در شبکه به NAT نیاز دارند.

تعداد ترجمه های همزمانی که یک روتر می تواند انجام دهد، ارتباط مستقیم با حافظه اصلی سیستم دارد. با توجه به اینکه در جدول ترجمه آدرس هر entry صرفا" ۱۶۰ بایت را اشغال خواهد کرد، یک روتر با ۴ مگابایت حافظه قادر به پردازش ۲۶.۲۱۴ ترجمه همزمان است. مقدار فوق برای اغلب موارد کافی بنظر می آید.

IANA محدوده ای از آدرس های IP را که غیرقابل روت بوده و شامل آدرس های داخلی شبکه هستند مشخص نموده است .آدرس های فوق غیرریجستر شده می باشند.. هیچ شرکت و یا آژانسی نمی تواند ادعای مالکیت آدرس های فوق را داشته باشد و یا آنها را در شبکه های عمومی (اینترنت) استفاده نماید. روترها بگونه ای طراحی شده اند که آدرس های فوق را عبور (Forward) نخواهند کرد.

- Range ۱: Class A - ۱۰.۰.۰.۰ through ۱۰.۲۵۵.۲۵۵.۲۵۵
- Range ۲: Class B - ۱۷۲.۱۶.۰.۰ through ۱۷۲.۳۱.۲۵۵.۲۵۵
- Range ۳: Class C - ۱۹۲.۱۶۸.۰.۰ through ۱۹۲.۱۶۸.۲۵۵.۲۵۵

همزمان با پیاده سازی یک NAT پویا، یک فایروال بصورت خودکار بین شبکه داخلی و شبکه های خارجی ایجاد می گردد. NAT صرفا" امکان ارتباط به کامپیوترهائی را که در حوزه داخلی می باشند را خواهد داد. این بدان معنی است که یک کامپیوتر موجود در خارج از شبکه داخلی ، قادر به ارتباط مستقیم با یک کامپیوتر موجود در حوزه داخلی نبوده ، مگر اینکه ارتباط فوق توسط کامپیوتر شما مقدار دهی اولیه (هماهنگی های اولیه از بعد مقداردهی آدرس های مربوطه) گردد. شما براحتی قادر به استفاده از اینترنت دریافت فایل و ... خواهید بود ولی افراد خارج از شبکه نمی توانند با استفاده از آدرس IP شما، به کامپیوتر شما متصل گردند. NAT ایستا ، امکان برقراری ارتباط با یکی از کامپیوترهای موجود در حوزه داخلی توسط دستگاههای موجود در خارج از شبکه را ، فراهم می نمایند.

برخی از روترهای مبتنی بر NAT امکان فیلترینگ و ثبت ترافیک را ارائه می دهند. با استفاده از فیلترینگ می توان سایت هائی را که پرسنل یک سازمان از آنها استفاده می نمایند را کنترل کرد.با ثبت ترافیک یک سایت می توان از سایت های ملاقات شده توسط کاربران آگاهی و گزارشات متعددی را بر اساس اطلاعات ثبت شده ایجاد کرد.

NAT دربرخی موارد با سرویس دهندگان Proxy ، اشتباه در نظر گرفته می شود. NAT و Proxy دارای تفاوت های زیادی می باشند. NAT بی واسطه بین کامپیوترهای مبداء و مقصد قرار می گیرد. Proxy بصورت بی واسطه نبوده و پس از استقرار بین کامپیوترهای مبداء و مقصد تصور هر یک از کامپیوترهای فوق را تغییر خواهد داد. کامپیوتر مبداء می داند که درخواستی را از Proxy داشته و می بایست بمنظور انجام عملیات فوق (درخواست) پیکربندی گردد. کامپیوتر مقصد فکر می کند که سرویس دهنده Proxy بعنوان کامپیوتر مبداء می باشد. Proxy در لایه چهارم (Transport) و یا بالاتر مدل OSI ایفای وظیفه می نماید در صورتیکه NAT در لایه سوم (Network) فعالیت می نماید. Proxy ، بدلیل فعالیت در لایه بالاتر در اغلب موارد از NAT کندتر است .

۷-۳: شبکه های خصوصی مجازی :

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 بمنظور برقراری ارتباط با دفاتر و نمایندگی در اقصی نقاط یک کشور و یا در سطح دنیا .

اکثر سازمانها و موسسات بمنظور 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)، (OC۳ (Optical Carrier-۳ (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 از خطوط 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(Network Virtual Private(VPN 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 بمنظور 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 Virtual private(VPDN dial-up network)، 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 Enterprise(ESP service provider) استفاده نمایند. سرویس دهنده ESP ، بمنظور نصب و پیکربندی VPN ، یک Network access server(NAS) را پیکربندی و نرم افزاری را در اختیار کاربران از راه دور بمنظور ارتباط با سایت قرار خواهد داد. کاربران در ادامه با برقراری ارتباط قادر به دستیابی به NAS و استفاده از نرم افزار مربوطه بمنظور 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 صورتیکه 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 بمنظور 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 بمنظور 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 بمنظور 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 بعنوان مسافر کشتی مسافربری بر روی سایر مسافرین حاضر در کشتی) .در صورتیکه 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 صورتیکه 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 صورتیکه 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 بمنظور 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 بمنظور تامین امنیت (داده ها و ارتباطات) از روش های متعددی استفاده می نمایند :

- فایروال : فایروال یک دیواره مجازی بین شبکه اختصاصی 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**
- **رمزنگاری کلید عمومی**

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 بمنظور رمزگشائی اطلاعات باشند. بمنظور 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 باطست تبدیل گردد. در چنین حالتی می باطست به دوست امین خود ، واقعیت فوق (کلید رمز) گفته شود. در صورتیکه 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. بمنظور 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 PGP(Pretty Good Privacy) است . با استفاده از روش فوق می توان اقدام به رمزنگاری اطلاعات دلخواه خود نمود.

- IPSec . پروتکل IPsec(protocol Internet protocol security) ، 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) بمنظور ایجاد امنیت بالا در محیط های 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 ") ، بمنظور 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 بمنظور سرویُس های Dial-up
- سرویس دهنده NAS که توسط مرکز ارائه خدمات اینترنت بمنظور 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 بمنظور 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 بمنظور 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(Private Internet eXchange) 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 بمنظور 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,L۲F,PPTP,L۲TP,GRE استفاده می گردد.

- پروتکل مسافر : از پروتکل هائی نظیر IPX,IP,NetBeui بمنظور 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(encapsulation generic routing) بعنوان 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 سایت 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 بعنوان 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 ۲ 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 .

Tunneling Protocol Point-to-Point(PPTP): پروتکل فوق توسط کنسرسیومی متشکل از شرکت های متفاوت ایجاد شده است . این پروتکل امکان رمزنگاری ۴۰ بیتی و ۱۲۸ بیتی را دارا بوده و از مدل های تعیین اعتبار کاربر که توسط PPP حمایت شده اند ، استفاده می نماید.

(L۲TP): پروتکل فوق با همکاری چندین شرکت ایجاد شده است .پروتکل فوق از ویژگی های PPTP و L۲F استفاده کرده است . پروتکل L۲TP بصورت کامل IPSec را حمایت می کند. از پروتکل فوق بمنظور ایجاد تونل بین موارد زیر استفاده می گردد :

- سرویس گیرنده و روتر
- NAS و روتر
- روتر و روتر

مشابه حمل یک کامپیوتر توسط یک کامیون است . فروشنده ، پس از بسته Tunnelingعملکرد 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.

WAP: Wireless Application Protocol

۳-۸ : WAP :

WAP درواقع جدیدترین شیوه ارائه اطلاعات برروی نوترین سیستم های موجودمی باشد. بطور خلاصه دراین تکنولوژی اطلاعات موجوددربسترهای مختلف ازطریق گوشی های تلفن همراه دریافت ویاارسال شده واطلاعات پس ازپردازش درسیستم های کامپیوتری مرتبط جهت دستیابی کاربران ،به عوض دریافت ازطریق کامپیوتربه تلفن های همراه انتقال مییابد. بنیانگذاراین تکنولوژی درابتداشرکت نوکیابوده که برای ایجاداین

بسترجدیدتاسطح تعریف پروتکل های مربوطه نیزاقدام نموده است . پس ازمعرفی تکنولوژی درابتداکلیه شرکت های بین المللی تولیدکننده تلفن همراه باایجادیک مجمع مشترک مبادرت به تصحیح وتاییدپروتکل های مربوطه درزمینه سرویس دهندگان اطلاعات وهمچنین نمایشگربرروی گوشی نمودندکه نهایتاًدرماه های اول سال ۱۹۹۹این تکنولوژی نهایی شده وبه تصویب رسید. درحال حاضرشرکت های موجوددراین کنسرسیوم به بیش از۲۰۰ شرکت مختلف که درگستره های مختلفی فعالیت دارندبالغ شده است که این امراهمیت این سرویس رانمایش می دهدWAP سرویسی است که اطلاعات موردنظرکاربر، به عوض دریافت ازاینترنت ونمایش برروی کامپیوترازطریق موبایل دریافت وباکمی محدودیت امکان ارسال ودریافت کلیه اطلاعات موردنظربرقرارمی گردد. بستراطلاعاتی به صورت Base Text بوده ودرمواردااستفاده کمترازابزارهای گرافیکی موجوددراینترنت استفاده می گردد. این امرازیک جهت به علت محدودیت نمایشگری گوشی بوده وازسوی دیگرذات اطلاعات نمایشی ، استفاده کمتری ازمحیط های گرافیکی به عمل می آورد. نسل آینده تلفن های همراه باتوجه به دراختیارداشتن صفحات نمایشی گرافیکی این محدودیت رانیزازبین برده ودرسال های آینده امیدمی رودکه کلیه اطلاعات ودرتمامی شاخه هابرروی صفحه نمایشگرموبایل به تصویرآورده شود.

بطورکلی بسترارسال ودریافت اطلاعات دراین تکنولوژی تفاوت چندانی باروش ارائه اطلاعات ازطریق اینترنت ودریافت ازطریق کامپیوترندارد‌خصوصاًتنظیماتی که کاربرمجبوراست جهت استفاده ازاین سیستم انجام دهدتغییری باروش استفاده ازاینترنت نداردازسوی دیگراطلاعات دریافتی هم می تواندبه شکل اطلاعات خصوصی برروی بستراینترنت به گوشی منتقل شودوهم توانایی این وجوددارد‌که اطلاعات ازطریق بسترارتباطی اینترنت دریافت ویاارسال گردد. امروزه هم سو باگسترش روزافزون شبکههای جهانی اطلاع رسانی برروی موبایل شبکه های خصوصی آن نیزحتی باسرعتی بیشتردرحال راه اندازی واستفاده می باشد.

فهرست استفاده های کلی این سیستم به شرح زیرمی باشد:

۱- اطلاعات خبری : اغلب شرکتهای بزرگ خبررسانی دنیاموازی باسایت اینترنتی خودسایت مخصوص موبایل نیزراه اندازی نموده اند.

۲- اطلاعات بورس : اغلب سرویس دهندگان بورس دردنیامبادرت به ارائه اطلاعات برروی تلفن همراه نموده اند. این امربه علت سرعت بالای تغییرات واهمیت دریافت سریع اطلاعات بسیارروبه گسترش می باشد

۳- اطلاعات بانکی : بانک های معتبردردنیاهمراه باسرویس های اضافه که به مشتریان خودمی دهنداطلاعات حساب های جاری مشتری رابه صورت Online ازطریق تلفن های همراه به افراد ارسال می دارند.حتی درمواردی امکان انتقالات مالی نیزازاین طریق ایجادشده است .

٤- اطلاعات علمی وفرهنگی . . . برای استفاده ازسرویس WAP درانتخاب گوشی تلفن همراه بایدتوجه لازم صورت پذیرد. مانندااستفاده ازاینترنت ازطریق کامپیوترکه درواقع کامپیوتربایدمسلح به یک مرورگرصفحات Web باشد(مانند Netscape,Ie) گوشی های قابل استفاده برای دریافت این سرویس نیزبایدمرورگر WAP رادراختیارداشته باشند. این سری ازگوشی هاازشش ماهه دوم سال ۱۹۹۹به شدت دربازارافزایش یافته اند. به طورکلی برای انتخاب گوشی ،بایدتوجه شودکه دردفترچه های راهنمای گوشی موردنظریکی ازمواردزیرذکرشده باشد: Active Internat Browser-Wap Enabled Service-Enabled Microbrowser-With Wap تمام گوشی های فوق دارای مودم داخلی خواهدبود. درصورتی که احتمالاً گوشی موردنظرمرورگر WAP راداشته امامودم نداشته باشد(که بعیدبه نظرمی رسد)می توان ازطریق مودم خارجی جهت ارتباط استفاده نمود.جهت ارتباط اینترنتی درداخل ایران بایدسرویس معروف به دیتاData ازمخابرات محلی تلفن همراه برای سیم کارت مربوط خریداری گردد. این سرویس به عنوان سرویس ویژه ازطریق مخابرات ارائه می گردد.به طورخلاصه هردستگاه تلفن همراه برای استفاده ازسرویس WAP بایددوامکان راداشته باشد:۱- مرورگر WAP داشته باشد.

۲- سرویس ویژه" دیتا" ازمخابرات گرفته شده باشد.

تنظیمات اساسی برروی گوشی برای ارتباط به شرح زیراست :

ـ درزمان تماس حتی المقدورشارژتلفن همراه حداکثرباشد. این امربه مودم داخلی این امکان رامی دهدکه ارتباط پایدارتری برقرارنماید.

- حتی المقدوردرمنطقه ای قراربگیریم که آنتن دهی تلفن همراه بسیاربالااست
- تنظیم Bearer که در کشور ایران حتما باید "" Data باشد.
- شماره تلفن سرویس دهنده در Dial up Number وارد شود.
- IP سرویس دهنده در سیستم معرفی گردد.
- ترجیحا سرعت ارتباطی Data Call Speed بر روی ۹۶۰۰ تنظیم گردد.

البته بالاترین سرعت ارتباطی مقدار ۱۴۴۰۰ می باشد که اغلب در خطوط تلفن ایران اتفاق نمی افتد. از روش Autobauding حتی المقدور استفاده نشود.

- نام کاربر و Password که از سرویس دهنده دریافت نموده اید درمحل خود وارد شود .
- برای ارتباط با سایت های اطلاعاتی مورد نظر آدرس سایت را باید در سیستم و در Bookmarks گوشی خود وارد کرده باشید. ترجیحاً حتماً در ابتدای آدرس http:// را وارد نمایید.

- پس از انجام تنظیمات در صورت انتخاب یک آدرس از Bookmark اتصال برقرار شده و پس از برقراری ارتباط اطلاعات بر روی صفحه تلفن همراه نمایش می یابد.

- در پایان ، لیست گوشی های قابل استفاده جهت سرویس WAP ارائه می شود .

۹-۳: مانیتورینگ دسترسی در ویندوز XP:

در ویندوز XP به راحتی می توانیم دسترسی به منابع را مانیتورینگ کنیم .با استفاده از مانیتورینگ شبکه می توانیم تعداد کاربرانی که از فایل ها و پوشه های اشتراکی استفاده می کنند را تعیین کنیم .همچنین می توانیم فایل های باز را بازبینی نماییم حتی قادر به قطع کردن ارتباط کاربران نیز خواهیم بود.می توانیم دسترسی یک کاربر به یک یا تعداد بیشتری از فایل های اشتراکی شبکه را قطع کنیم .

بسیار مهم است که شما بعنوان یک مدیر شبکه دلایل لزوم اجرای مانیتورینگ بر روی کامپیوترهای شبکه تان را بدانید.برخی از این دلایل در زیر آورده شده است :

نگهداری از منابع : شما بعنوان مدیر شبکه باید بدانید کدامیک از کاربران بطور مداوم از منابع استفاده می کنند .

امنیت : یک مدیر شبکه باید منابع محرمانه را از دسترس عموم کاربران دور نگه دارد و تنها به کاربرانی که اجازه دسترسی به این منابع را دارند امکان استفاده از آنها را دهد .

برنامه ریزی : باید تعیین کنیم که کدام منبع و به چه میزان مورد استفاده قرار می گیرد بنابراین می توانیم برای افزایش منابع در سیستم آینده برنامه ریزی کنیم .

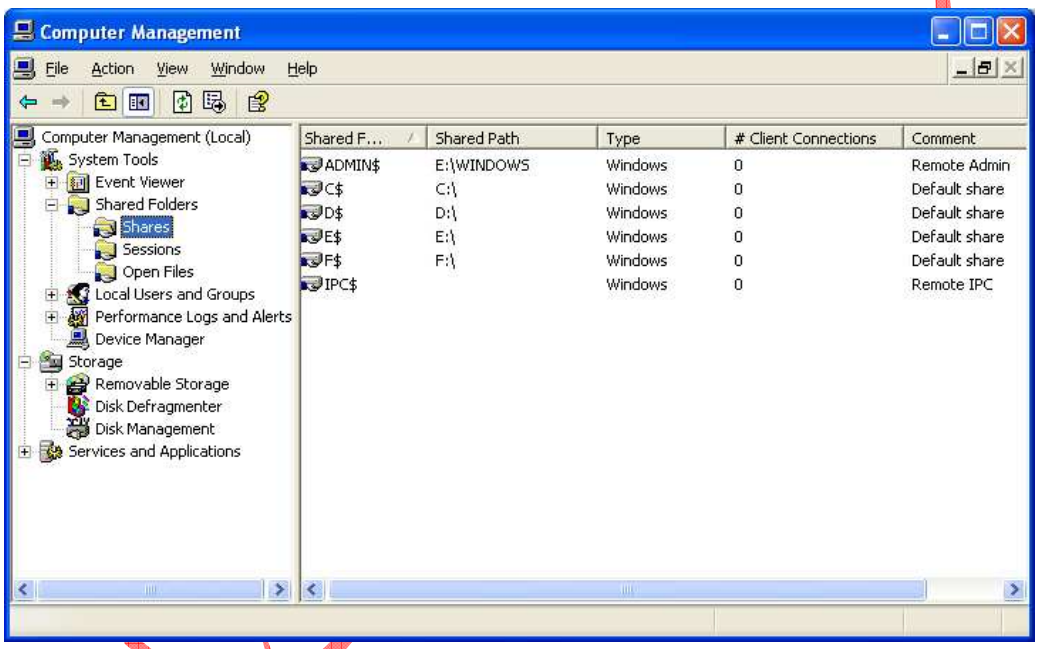
آنچه برای مانیتورینگ منابع شبکه نیاز است :

در یک شبکه تمامی کاربران نمی توانند منابع اشتراکی را مانیتور کنند ،تنها گروه خاصی قادر به انجام اینکار می باشند.جدول زیر این گروه ها را مشخص می کند .

کامپیوترهایی که می توانند مدیریت کنند	نام گروه ها
همه کامپیوترهای دامنه مربوطه	مدیران کاربران سروردر دامنه خاص
کامپیوترهای محلی ویا راه دور در یک گروه کاری	مدیران و یا کاربرانی که سیستم XP Professional دارند.

مانیتورینگ فولدرهای اشتراکی :

صفحه ای که در شکل زیر نشان داده شده مربوط به Computer Management می باشد .شما در این صفحه می توانید لیست فولدرهای اشتراکی را ببینید.



شکل ۱۶-۳

در جدول صفحه زیر توضیحات مختصری راجع به هر یک از ستونهای Computer Management آورده شده است .

نام ستون	توضیحات
Shared Folder	فولدر های اشتراکی روی سیتم را با نامی که زمان به اشتراک گذاشتن به آن داده اید ،نشان می دهد.
Shared Path	مسیر فولدر اشتراکی بر روی هارد را نشان میدهد.
Type	نوع اتصال شبکه را نشان می دهد: Microsoft Windows ، Novell ، NetWare یا Apple Macintosh .
#Client Connection	تعداد کلاینت هایی را که از فولدرهای اشتراکی استفاده کردهاند را نشان می دهد .
Comment	شامل توضیحی مختصر راجع به فولدریست که به اشتراک گذاشته شده است.

نکته :ویندوز XP بطور اتوماتیک لیست فولدرهای اشتراکی و فایلهای باز را update نمی کند .برای اینکار لازم است از منوی Action گزینه Refresh را انتخاب کنید .

تعیین تعداد کاربرانی که می توانند به فایلهای اشتراکی بطورهمزمان دسترسی داشته باشند :

میتوان ماگزیمم تعداد کاربرانی که می توانند از منابع اشتراکی بطور همزمان استفاده کنند را تعیین کرد. برای اینکار از لیست Shared Folders فولدر مورد نظرتان را انتخاب کنید .سپس از منوی

Action ، Properties را انتخاب نمایید .پنجره مشخصات فولدر مورد نظر باز خواهد شد . General محدوده کاربر را نشان می دهد .در ویندوز XP ماگزیمم ۱۰ می باشد ،اما می توان آن را روی عددی کمتر تنظیم کرد .

تغییر دادن مشخصات فولدر اشتراکی :

شما می توانید تغییراتی را در فولدر های اشتراکی موجود ایجاد کنید ،این تغییرات می تواند شامل تغییر نام فولدر ،ویا تغییر مجوزها باشد . برای تغییر ویژگیها ی یک فولدر ، روی نام آن کلیک کنید سپس از منوی Action ، Properties را انتخاب کنید . General ، نام فولدر،مسیر آن و توضیحات مربوط به فولدر مورد نظر را نشان می دهد . General همچنین به شما کمک میکند تا مجوزهای دسترسی کاربران را ببینید و تغییر دهید .

مانیتورینگ فایل های باز :

با بکار گیری فولدر Open File در Computer Management می توانید فایل های باز و کاربران آنها را ببینید .

قطع ارتباط کاربران از فایل های باز :

میتوانید ارتباط کاربر یا کاربران را از فایل اشتراکی که در حال اجراست قطع کنید . اگر تغییراتی درمجوزهای NTFSیک فایل ایجاد کرده باشید و کاربری در حال استفاده از همان فایل باشد ، تا زمانی که کاربر مذکور فایل را نبسته واقدام به استفاده مجدد از آن را ننماید ،این تغییرات شامل حال وی نمی شود .

می توانید این تغییرات را به دو روش زیر اعمال نمایید :

ارتباط تمام کاربران را با کلیه فایلهای در حال اجرا قطع کنید :برای اینکار Open Files را باز کرده و سپس از منوی Action ، Disconnect All Open Files را انتخاب نمایید .

دسترسی همه کاربران به یک فایل را قطع کنید : برای اینکار لازم است از منوی Open Files فایل مورد نظر را انتخاب کرده و سپس از منوی Action ، Close Open File را انتخاب کنید .

۳-۱۰ : شبکه نوری SONET Synchronous optical Network

SONET یک حملکننده نوری با سرعت بالاست که از کابل فیبر نوری به عنوان رسانه انتقال استفاده میکند. واژهSONET عبارتست از استانداردی که توسط موسسه ANSI وضع شده است. اتحادیهITU استانداردی برایSONET وضعنموده وآنرا -SDH Synchronous Digital Hierarchy نامید که در اروپا مورد استفادهقرار میگیرد.

معماری نوریSONET براساس چهار فیبر نوری با حلقهای دردو جهت طراحی میشود تاسرویسهایی باحداکثر اطمینان را ارائه نماید. نرمافزارهای کاربردی جدید مثلCADCAMوMedia Image به پهنای باند و سیعتری نسبت به دیگر نرمافزارهای کاربردی نیاز دارند و SONETپهنای باندی گسترده و با سرعت ارسال بالایی را ارائه میدهد.

مشخصات SONET :

- SONET برای کلیه سطوح از روش مالتی پلکس کردن (تسهیمسازی) بایت استفاده میکند.
- SONET یک فنآوری با سرعت بالاست که دارای ویژگی اصلاح خودکار مسیر (Self-Correcting Path) میباشد.
- SONETروش مالتیپلکس کردن ودیمالتیپلکس کردن را به کار میبرد.
- سیگنال الکتریکی پایه برایSONET عبارتست ازSTS-۱(سیگنالهای حامل سنکرون سطح یک)
- SONET با سرعت۸۰۰۰ فریم در ثانیهSTS-۱ را ارسال میکند.
- سیگنالهای کندتر میتواند بر روی سیگنالهای سریعتر مستقیما" مولتیپلکس شوند.

اجزاء SONET:

شامل یک مالتیپلکس کنندهSTS و یک بازمولد(Regenerator)، یک مالتیپلکسکننده حذف/اضافه، یک مبدل سیگنا ل الکتریکی به سیگنال نوری(E/O) و یک دیمالتیپلکس کنندهSTSاست.

مالتیپلکسر:STS وظیفه یکSTS-MUXعبارتست از: مولتیپلکسکردن سیگنالهایالکتریکی ورودی به دادههایی با سرعت بالاتر و نهایتا" تبدیل نتایج به سیگنالهای نوری.

بازمولد(: (Regenerator بازمولد وظیفه تکرارکننده را انجام میدهد. اگر کابل نوری از طول استاندارد بلندتر باشد، از بازمولد برای دریافت سیگنالهای نوری و تقویت مجدد آن سیگنالهای نوری استفاده میشود.

مالتیپلکسر حذفکننده/اضافه کننده(Add/Drop Multi Pelexer) : این مالتیپلکسر برای استخراجکردن ویا درجکردن سیگنالهای با سرعتپائین و یا به سیگنالهای مولتیپلکسشده با سرعت بالا بکار میرود. این عمل بدون دیمالتیپلکسکردن کامل سیگنالهایSONET انجام میشود.

دیمالتیپلکسرSTS: این دیمالتیپلکس کننده، سیگنالهای نوری را به سیگنالهای الکتریکی تبدیل نموده و آنها را برای استفاده کنندگان دیمالتیپلکس می کند.

.

ADSL چیست ؟

ADSL یا خط دیجیتالی نامتقارن، به نوعی ارتباط پرسرعت دیتا جهت دسترسی به اینترنت و یا پخش ویدئویی اطلاق می گردد که از طریق خطوط تلفن معمولی انجام می پذیرد. ADSL درواقع یکی از انواع خدمات و محصولات xDSL می باشد که به منظور انتقال پرسرعت دیتا تا Mbps ۲ بر روی سیم تلفن مسی موجود در شبکه تلفنی (PSTN) طراحی گردیده است.

مزایای استفاده از سرویس ADSL

• دسترسی به اینترنت پرسرعت

• اتصال دائم به اینترنت

• استفاده همزمان از اینترنت و تلفن

• حق اشتراک ثابت ماهانه

• نصب سریع و آسان

شیوه ای نوین برای برقراری ارتباط با اینترنت :

تکنولوژی جدید ADSL (Asymmetric Digital Subscriber Line) با ارتقاء امکانات خطوط تلفن آنالوگ، انتقال پرسرعت داده ها را همزمان با انتقال صوت امکان پذیر نموده است. در روش ADSL (خط دیجیتالی نامتقارن مشترک) برخلاف روش Dialup موجود، سیگنالهای دیجیتالی به صوتی تبدیل نمی شوند و کانال انتقال Data از Voice کاملا" مجزا می باشد. بنابراین کاربر بدون نیاز به خط تلفن جدید حین ارتباط با اینترنت قادر به برقراری مکالمات تلفنی نیز خواهد بود.

ارتباطی پرسرعت با اینترنت :

روشADSL ندا، ارتباط با اینترنت را با سرعتی تا ۳۰ برابر روشهای Dialup برای کاربران امکان پذیر نموده است که البته میزان سرعت به نسبت تعداد کاربران محلی online از ۶۴Kb/s تا ۱ Mb/s متغیر می باشد.

سرویس ADSL باتوجه به سرعت بالای ارتباط (در مقایسه با سرویس های Dialup) و هزینه مناسب (در مقایسه با سرویس های پهنای باند موجود) راه کاری ایده آل برای کاربران خانگی پرمصرف و کاربران تجاری (دارای شبکه داخلی) می باشد.

اتصال دائمی به شبکه اینترنت :

در روش ارتباطی ADSL کامپیوتر یا کل شبکه داخلی شما در اتصال دائم با شبکه جهانی اینترنت می باشد. بدون انجام شماره گیری، بدون شنیدن بوق اشغالی و بدون اتلاف وقت جهت برقراری ارتباط، فقط با روشن کردن کامپیوتر به دنیای اینترنت قدم بگذارید. با بهره گیری از سرویس ADSL در عصر پرسرعت تبادل اطلاعات وقت و هزینه های خود را بیهوده هدر نمی دهید.

بدون هزینه های تلفن و هزینه های پنهان :

باتوجه به تقسیم خط تلفن به دو بخش انتقال Voice و Data توسط تکنولوژی ADSL، برقراری ارتباط با شبکه اینترنت بدون پرداخت هزینه تلفن میسر گردیده است. با سرویس ADSL بدون هیچ نگرانی از پرداخت هزینه های سنگین تلفنی و تنها با پرداخت حق اشتراک ثابت ماهانه، صرفنظر از میزان استفاده، از اتصالی مطمئن به اینترنت لذت ببرید.

را ه اندازی سریع و آسان :

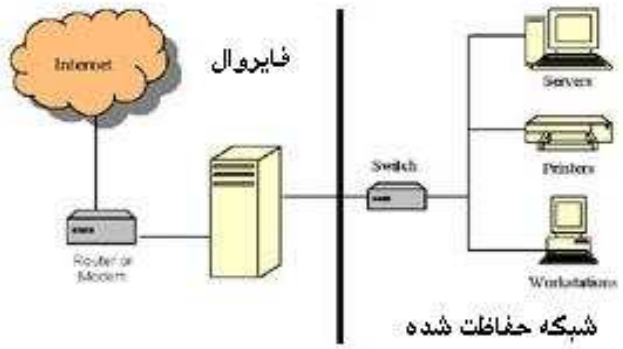
راه اندازی سرویس ADSL در مقایسه با ارتباط بی سیم نقطه به نقطه، P۲P و Line Leased بسیار سریعتر و ساده تر بوده و ظرف مدت کوتاهی انجام می گیرد. تکنولوژی ADSL کامپیوتر شما در اندک زمانی به عضوی از شبکه اینترنت مبدل می نماید.

فصل چهارم

امنیت شبکه

۴-۱ : فایروال :

در صورتیکه تاکنون مدت زمان کوتاهی از اینترنت استفاده کرده باشید و یا در یک اداره مشغول بکار هستید که بستر لازم برای دستیابی به اینترنت فراهم شده باشد، احتمالا" واژه " فایروال " را شنیده اید. مثلا" اغلب گفته می شود که : " در اداره ما امکان استفاده از این سایت وجود ندارد ، چون سایت فوق را از طریق فایروال بسته اند " . در صورتیکه از طریق خط تلفن به مرکز ارائه دهنده خدمات اینترنت (ISP) متصل و از اینترنت استفاده می نمائید ، امکان استفاده فایروال توسط ISP مربوطه نیز وجود دارد. امروزه در کشورهائی که دارای خطوط ارتباطی با سرعت بالا نظیر DSL و یا مودم های کابلی می باشند ، به کاربران خانگی توصیه می گردد که هر یک از فایروال استفاده نموده و با استقرار لایه فوق بین شبکه داخلی در منزل و اینترنت ، مسائل ایمنی را رعایت نمایند. بدین ترتیب با استفاده از یک فایروال می توان یک شبکه را در مقابل عملیات غیر مجاز توسط افراد مجاز و عملیات مجاز توسط افراد غیرمجاز حفاظت کرد.



شکل ۴-۱

فایروال چیست ؟

فایروال نرم افزار و یا سخت افزاری است که اطلاعات ارسالی از طریق اینترنت به شبکه خصوصی و یا کامپیوتر شخصی را فیلتر می نماید. اطلاعات فیلترشده ، فرصت توزیع در شبکه را بدست نخواهند آورد.

فرض کنید، سازمانی دارای ۵۰۰ کارمند باشد. سازمان فوق دارای ده ها کامپیوتر بوده که بر روی هر کدام یک کارت شبکه نصب شده و یک شبکه درون سازمانی (خصوصی) ایجاد شده است . سازمان فوق دارای یک یا چند خط اختصاصی (۱T و یا T۳) برای استفاده از اینترنت است . بدون استفاده از فایروال تمام کامپیوترهای موجود در شبکه داخلی، قادر به ارتباط با هر سایت و هر شخص بر روی اینترنت می باشند. کاربران مربوطه قادر به استفاده از برنامه هائی همچون FTP و یا Telnet بمنظور ارتباط مستقیم با افراد حقوقی و یا حقیقی موجود بر روی اینترنت می باشند. عدم رعایت مسائل ایمنی توسط پرسنل سازمان، می تواند زمینه دستیابی به اطلاعات موجود در شبکه داخلی را برای سارقین و متجاوزان اطلاعاتی اینترنت فراهم نماید.

زمانیکه در سازمان فوق از فایروال استفاده گردد، وضعیت کاملا" تغییر خواهد کرد. سازمان مربوطه می تواند برروی هر یک از خطوط ارتباطی اینترنت یک فایروال نصب نماید.فایروال مجموعه سیاست های امنیتی را پیاده سازی می نماید. مثلا" یکی از قوانین فوق می تواند بصورت زیر باشد :

- تمام کامپیوترهای موجود در شبکه مجاز به استفاده از اینترنت می باشند ، فقط یک فرد مجاز به استفاده از سرویس FTP است و سایر پرسنل مجاز به استفاده از سرویس فوق نخواهند بود.

یک سازمان می تواند برای هر یک از سرویس دهندگان خود (وب ، FTP، Telnet و ...) قوانین مشابه تعریف نماید. سازمان قادر به کنترل پرسنل بهمراه لیست سایت های مشاهده خواهد بود. با استفاده از فایروال یک سازمان قادر به کنترل کاربران شبکه خواهد بود .

فایروال ها بمنظور کنترل ترافیک یک شبکه از روش های زیر استفاده می نمایند:

- فیلتر نمودن بسته های اطلاعاتی . بسته های اطلاعاتی با استفاده ازتعدادی فیلتر، آنالیز خواهند شد. بسته هائی که از آنالیز فوق سربلند بیرون آیند از فایروال عبور داده شده و بسته ها ئی که شرایط لازم را برای عبور از فایروال را نداشته باشند دور انداخته شده و از فایروال عبور نخواهند کرد.

- سرویس Proxy . اطلاعات درخواستی از طریق اینترنت توسط فایروال بازیابی و در ادامه در اختیار درخواست کننده گذاشته خواهد شد. وضعیت فوق در مواردیکه کامپیوتر موجود در شبکه داخلی، قصد ارسال اطلاعاتی را برای خارج از شبکه خصوصی داشته باشند ، نیز صدق می کند.

بهینه سازی استفاده از فایروال:

فایروال ها را می توان با توجه به اهداف سازمانی بصورت کاملا" سفارشی نصب و پیکربندی کرد. در این راستا امکان اضافه و یا حذف فیلترهای متعدد بر اساس شرایط متفاوت وجود خواهد داشت :

- آدرس های IP . هر ماشین بر روی اینترنت دارای یک آدرس منحصر بفرد با نام IP است . IP یک عدد ۳۲ بیتی بوده که بصورت چهار عدد دهدهی که توسط نقطه از هم جدا می گردند نمایش داده می شود (Octet) . در صورتیکه یک آدرس IP خارج از شبکه، فایل های زیادی را از سرویس دهنده می خواند (ترافیک و حجم عملیات سرویس دهنده را افزایش خواهد داد) فایروال می تواند ترافیک از مبداء آدرس فوق و یا به مقصد آدرس فوق را بلاک نماید.

- اسامی دامنه ها (حوزه) . تمام سرویس دهندگان بر روی اینترنت دارای اسامی منحصر بفرد با نام " اسامی حوزه" می باشند. یک سازمان می تواند با استفاده از فایروال، دستیابی به سایت هائی را غیرممکن و یا صرفا" امکان استفاده از یک سایت خاص را برای پرسنل خود فراهم نماید.

- پروتکل ها . پروتکل نحوه گفتگوی بین سرویس دهنده و سرویس گیرنده را مشخص می نماید . پروتکل های متعدد با توجه به اهداف گوناگون در اینترنت استفاده می گردد. مثلا" http پروتکل وب و Ftp پروتکل مربوط به دریافت و یا ارسال فایل ها است . با استفاده از فایروال می توان، میدان فیلتر نمودن را بر روی پروتکل ها متمرکز کرد. برخی از پروتکل های رایج که می توان بر روی آنها فیلتر اعمال نمود بشرح زیر می باشند :

- (IP)(Internet Protocol) پروتکل اصلی برای عرضه اطلاعات بر روی اینترنت است .
- (TCP)(Protocol Transport Control) مسئولیت تقسیم یک بسته اطلاعاتی به بخش های کوچکتر را دارد.
- (HTTP) (Hyper Text Transfer Protocol) . پروتکل فوق برای عرضه اطلاعات در وب است.
- (FTP)(File Transfer Protocol). پروتکل فوق برای دریافت و ارسال فایل ها استفاده می گردد.
- (UDP)(User Datagram Protocol). از پروتکل فوق برای اطلاعاتی که به پاسخ نیاز ندارند استفاده می شود(پخش صوت و تصویر)
- (ICMP)(Internet control Message Protocol). پروتکل فوق توسط روترها و بمنظور تبادل اطلاعات فی المابین استفاده می شود.
- (SMTP)(Simple Mail Transfer Protocol) . از پروتکل فوق برای ارسال e-mail استفاده می گردد.
- (SNMP)(Simple Network Management Protocol)از پروتکل فوق بمنظور اخذ اطلاعات از یک کامپیوتر راه دور استفاده میشود
- Telnet . برای اجرای دستورات بر روی یک کامپیوتر از راه دور استفاده می گردد.

- پورت ها . هر سرویس دهنده ، خدمات مورد نظر خود را با استفاده از پورت های شماره گذاری شده بر روی اینترنت ارائه می دهد. مثلا" سرویس دهنده وب اغلب از پورت ۸۰ و سرویس دهنده Ftp از پورت ۲۱ استفاده می نماید. یک سازمان ممکن است با استفاده از فایروال امکان دستیابی به پورت ۲۱ را بلاک نماید.

- کلمات و عبارات خاص . می توان با استفاده از فایروال کلمات و یا عباراتی را مشخص نمود تا امکان کنترل بسته های اطلاعاتی حاوی کلمات و عبارات فراهم گردد. هر بسته اطلاعاتی که حاوی کلمات مشخص شده باشد توسط فایروال بلاک خواهد شد.

همانگونه که اشاره شد فایروال ها به دو صورت نرم افزاری وسخت افزاری استفاده می گردند.فایروال های نرم افزاری بر روی کامپیوتری نصب می گردند که خط اینترنت به آنها متصل است .کامپیوتر فوق بمنزله یک Gateway رفتار می نماید چون تنها نقطه قابل تماس، بمنظور ارتباط کامپیوتر و اینترنت است . زمانیکه فایروال بصورت سخت افزاری در نظر گرفته شود ، تمام بخش فوق بصورت Gateway خواهد بود. امنیت فایروال های سخت افزاری بمراتب بیشتر از فایروال های نرم افزاری است .

تهد یدات :

حمله کنندگان به شبکه های کامپیوتری از روش های متعددی استفاده می نمایند.

- Remote Login . امکان برقراری ارتباط با کامپیوتر و کنترل آن توسط فرد غیرمجاز است . دامنه عملیات فوق می تواند از مشاهده و دستیابی به برخی از فایل ها تا اجرای برخی برنامه ها بر روی کامپیوتر باشد.

-Application Backdoors . برخی از برنامه ها دارای امکانات ویژه ای برای دستیابی از راه دور می باشند. برخی دیگر از برنامه ها دارای اشکالاتی بوده بگونه ای که یک Backdoor را ایجاد و یا امکان دستیابی مخفی را ارائه می دهند. در هر حالت امکان کنترل برنامه فراهم خواهد گردید.

- SMTP session hijacking . پروتکل SMTP رایج ترین روش برای ارسال e-mail است . با دستیابی به لیستی از آدرس های e-mail ، یک شخص قادر به ارسال e-mail به هزاران کاربر دیگر خواهد شد.

- اشکالات سیستم های عامل . سیستم های عامل نظیر سایر برنامه های کاربردی ممکن است دارای Backdoors باشند.

- انفجار E-mail . یک شخص قادر به ارسال صدها و هزاران e-mail مشابه در مقاطع زمانی متفاوت است . با توجه به وضعیت فوق سیستم پست الکترونیکی قادر به دریافت تمام نامه های ارسالی نخواهد بود.

- ماکرو. اغلب برنامه های کاربردی این امکان را برای کاربران خود فراهم می نمایند که مجموعه ای از اسکریپت ها را بمنظور انجام عملیات خاصی نوشته و نرم افزار مربوطه آنها را اجراء نماید. اسکریپت های فوق " ماکرو "نامیده می شوند. حمله کنندگان به شبکه های کامپیوتری با آگاهی از واقعیت فوق، اقدام به ایجاد اسکریپت های خاص خود نموده که با توجه به نوع برنامه ممکن است داده ها را حذف و یا باعث از کار افتادن کامپیوتر گردند.

- ویروس . رایج ترین روش جهت آسیب رساندن به اطلاعات، ویروس است . ویروس یک برنامه کوچک است که قادر به تکثیر خود بر روی کامپیوتر دیگر است . عملکرد ویروس ها بسیار متفاوت بوده و از اعلام یک پیام ساده تا حذف تمام داده ها را می تواند شامل گردد.

سرویس دهنده Proxy :

سرویس دهنده Proxy اغلب با یک فایروال ترکیب می گردد. سرویس دهنده Proxy بمنظور دستیابی به صفحات وب توسط سایر کامپیوترها استفاده می گردد. زمانیکه کامپیوتری درخواست یک صفحه وب را می نماید، صفحه مورد نظر توسط سرویس دهنده Proxy بازیابی و در ادامه برای کامپیوتر متقاضی ارسال خواهد شد. بدین ترتیب تمام ترافیک (درخواست و پاسخ) بین درخواست کننده یک صفحه وب و پاسخ دهنده از طریق سرویس دهنده Proxy انجام می گیرد.

سرویس دهنده Proxy می تواند کارائی استفاده از اینترنت را افزایش دهد. پس از دستیابی به یک

صفحه وب ، صفحه فوق بر روی سرویس دهنده Proxy نیز ذخیره (Cache) می گردد. در صورتیکه در آینده قصد استفاده از صفحه فوق را داشته باشید صفحه مورد نظر از روی سرویس دهنده Proxy در اختیار شما گذاشته می شود.

(الزامی به برقراری ارتباط مجدد و درخواست صفحه مورد نظر نخواهد بود).

نتیجه گیری

برای یک تکنسین شبکه دانستن اینکه کامپیوتر ها چطور با یکدیگر در یک شبکه کامپیوتری ارتباط برقرار می کنند بسیار مهم می باشد .

این روزها استفاده از کامپیوترها در یک Settingخاص و حرفه ای بدون وجود شبکه تصور کردنی نیست. تکنسینهای شبکه باید تمامی ملزومات یک شبکه کامپیوتری را بدانند وبر نگهداری و اشکال زدایی شبکه های خود مسلط باشند.

فهرست مراجع : **نام مولف:**

Microsoft Windows XP Professional — Rick Wallace

Windows ۲۰۰۰ Active Directory Services — Microsoft Corporation

Network+