شبکه

شبکه اترنت

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

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

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

شبکه های محلی و شبکه های گسترده

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

اترنت

در سال ۱۹۷۳ پژوهشگری با نام " Metcalfe" در مرکز تحقیقات شرکت زیراکس، اولین شبکه اترنت را بوجود آورد.هدف وی ارتباط کامپیوتر به یک چاپگر بود. وی روشی فیزیکی بمنظور کابل کشی بین دستگاههای متصل بهم در اترنت ارائه نمود. اترنت در مدت زمان کوتاهی بعنوان یکی از تکنولوژی های رایج برای برپاسازی شبکه در سطح دنیا مطرح گردید. همزمان با پیشرفت های مهم در زمینه شبکه های کامپیوتری ، تجهیزات و دستگاه های مربوطه، شبکه های اترنت نیز همگام با تحولات فوق شده و قابلیت های متفاوتی را در بطن خود ایجاد نمود. با توجه به تغییرات و اصلاحات انجام شده در شبکه های اترنت ،عملکرد و نحوه کار آنان نسبت به شبکه های اولیه تفاوت چندانی نکرده است . در اترنت اولیه، ارتباط تمام دستگاه های موجود در شبکه از طریق یک کابل انجام می گرفت که توسط تمام دستگاهها به اشتراک گذاشته می گردید. پس از اتصال

یک دستگاه به کابل مشترک ، می بایست پتانسیل های لازم بمنظور ایجاد ارتباط با سایر دستگاههای مربوطه نیز در بطن دستگاه وجود داشته باشد (کارت شبکه) . بدین ترتیب امکان گسترش شبکه بمنظور استفاده از دستگاههای چدید براحتی انجام و نیازی به اعمال تغییرات بر روی دستگاههای موجود در شبکه نخواهد بود.

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

پروتکل

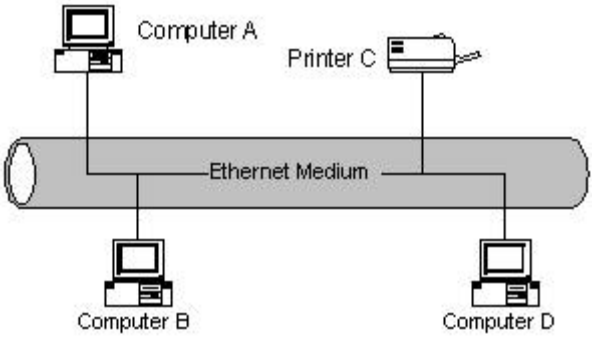
پروتکل در شبکه های کامپیوتری به مجموعه قوانینی اطلاق می گردد که نحوه ارتباطات را قانونمند می نماید. نقش پروتکل در کامپیوتر نظیر نقش زبان برای انسان است . برای مطالعه یک کتاب نوشته شده به فارسی می بایست خواننده شناخت مناسبی از زبان فارسی را داشته باشد. بمنظور ارتباط موفقیت آمیز دو دستگاه در شبکه می بایست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

اصطلاحات اترنت

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

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

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



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

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

CSMA/CD

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

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

Carrier-sense multiple access شروع یک گفتگو را قانونمند و تنظیم می نماید ولی در این رابطه یک نکته دیگر وجود دارد که می بایست برای آن نیز راهکاری اتخاذ شود.فرض کنید در مثال میز ناهار خوری در یک لحظه سکوتی حاکم شود و دو نفر نیز قصد حرف زدن را داشته باشند.در چنین حالتی در یک لحظه سکوت

موجود توسط دو نفر تشخیص و بلافاصله هر دو تقریبا" در یک زمان یکسان شروع به حرف زدن می نمایند.چه اتفاقی خواهد افتاد ؟ در اترنت پدیده فوق را تصادم (Collision) می گویند و زمانی اتفاق خواهد افتاد که دو ایستگاه قصد استفاده از محیط انتقال و ارسال اطلاعات را بصورت همزمان داشته باشند. در گفتگوی انسان ها ، مشکل فوق را می توان بصورت کاملا" دوستانه حل نمود. ما سکوت خواهیم کرد تا این شانس به سایرین برای حرف زدن داده شود.همانگونه که در زمان حرف زدن من، دیگران این فرصت را برای من ایجاد کرده بودند! ایستگاههای اترنت زمانیکه قصد ارسال اطلاعات را داشته باشند، به محیط انتقال گوش فرا داده تا به این اطمینان برسند که تنها ایستگاه موجود برای ارسال اطلاعات می باشند. در صورتیکه ایستگاههای ارسال کننده اطلاعات متوجه نقص در ارسال اطلاعات خود گردند ،از بروز یک تصادم در محیط انتقال آگاه خواهند گردید. در زمان بروز تصادم ، هر یک از ایستگاههای مربوطه به مدت زمانی کاملا" تصادفی در حالت انتظار قرار گرفته و پس از اتمام زمان انتظار می بایست برای ارسال اطلاعات شرط آزاد بودن محیط انتقال را بررسی نمایند! توقف تصادفی و تلاش مجدد یکی از مهمترین بخش های پروتکل است .

محدودیت های اترنت

یک شبکه اترنت دارای محدودیت های متفاوت از ابعاد گوناگون (بکارگیری تجهیزات) است .طول کابلی که تمام ایستگاهها بصورت اشتراکی از آن بعنوان محیط انتقال استفاده می نمایند یکی از شاخص ترین موارد در این زمنیه است . سیگنال های الکتریکی در طول کابل بسرعت منتشر می گردند. همزمان با طی مسافتی، سیگنال ها ضعیف می گردند. وجود میدان های الکتریکی که توسط دستگاههای مجاور کابل نظیر لامپ های فلورسنت ایجاد می گردد ، باعث تلف شدن سیگنال می گردد. طول کابل شبکه می بایست کوتاه بوده تا امکان دریافت سیگنال توسط دستگاه های موجود در دو نقطه ابتدائی و انتهائی کابل بصورت شفاف و با حداقل تاخیر زمانی فراهم گردد. همین امر باعث بروز محدودیت در طول کابل استفاده شده، می گردد

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

تولید کنندگان تجهیزات شبکه دستگاه های متفاوتی را بمنظور غلبه بر مشکلات و محدودیت گفته شده ، طراحی و عرضه نموده اند. اغلب دستگاههای فوق مختص شبکه های اترنت نبوده ولی در سایر تکنولوژی های مرتبط با شبکه نقش مهمی را ایفاء می نمایند.

تکرارکننده (Repeater)

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

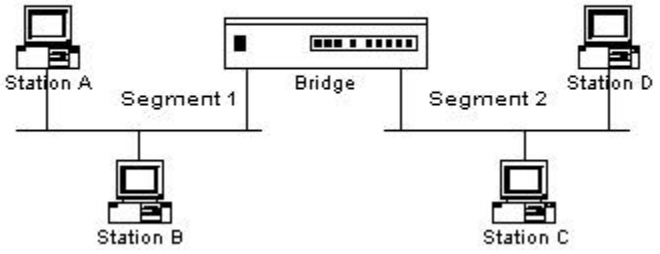
Bridges و سگمنت

شبکه های اترنت همزمان با رشد (بزرگ شدن) دچار مشکل تراکم می گردند. در صورتیکه تعداد زیادی ایستگاه به یک سگمنت متصل گردند، هر یک دارای ترافیک خاص خود خواهند بود . در شرایط فوق ،

ایستگاههای متعددی قصد ارسال اطلا عات را دارند ولی با توجه به ماهیت این نوع از شبکه ها در هر لحظه یک ایستگاه شانس و فرصت استفاده از محیط انتقال را پیدا خواهد کرد. در چنین وضعیتی تعداد تصادم در شبکه افزایش یافته و عملا" کارآئی شبکه افت خواهد کرد. یکی از راه حل های موجود بمنظور برطرف نمودن مشکل تراکم در شبکه تقسیم یک سگمنت به چندین سگمنت است . با این کار برای تصادم هائی که در شبکه بروز خواهد کرد، دامنه وسیعتری ایجاد می گردد.راه حل فوق باعث بروز یک مشکل دیگر می گردد: سگمنت ها قادر به اشتراک اطلاعات با یکدیگر نخواهند بود.

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

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



همانگونه که در شکل فوق مشاهده می گردد Bridge دو سگمنت را به یکدیگر متصل نموده است . در صورتیکه ایستگاه A و یا B قصد ارسال اطلاعات را داشته باشند Bridge نیز فریم های اطلاعاتی را دریافت خواهد کرد. نحوه برخورد Bridge با فریم های اطلاعاتی دریافت شده به چه صورت است؟ آیا قادر به ارسال اتوماتیک فریم ها برای سگمنت دوم می باشد؟ یکی ازاهداف استفاده از Bridge کاهش ترافیک های غیرضروری در هر سگمنت است . در این راستا، آدرس مقصد فریم ، قبل از هر گونه عملیات بر روی آن، بررسی خواهد شد. در صورتیکه آدرس مقصد، ایستگاههای A و یا B باشد نیازی به ارسال فریم برای سگمنت شماره دو وجود نخواهد داشت . در این حالت Bridge عملیات خاصی را انجام نخواهد داد. نحوه برخورد Bridge با فریم فوق مشابه فیلتر نمودن است . درصورتیکه آدرس مقصد فریم یکی از ایستگاههای C و یا D باشد و یا فریم مورد نظر دارای یک آدرس از نوع Broadcast باشد ، Bridge فریم فوق را برای سگمنت شماره دو ارسال خواهد کرد. با ارسال و هدایت فریم اطلاعاتی توسط Bridge امکان ارتباط چهار دستگاه موجود در شبکه فراهم می گردد. با توجه به مکانیزم فیلتر نمودن فریم ها توسط Bridge ، این امکان بوجود خواهد آمد که ایستگاه A اطلاعاتی را برای ایستگاه B ارسال و در همان لحظه نیز ایستگاه C اطلاعاتی را برای ایستگاه D ارسال نماید.بدین ترتیب امکان برقراری دو ارتباط بصورت همزمان بوجود آمده است .

روترها : سگمنت های منطقی

با استفاده از Bridge امکان ارتباط همزمان بین ایستگاههای موجود در چندین سگمنت فراهم می گردد. Bridge

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

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

وضعیت فعلی اترنت

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

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

اترنت و استاندارد ۸۰۲,۳

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

۸۰۲,۳ از نظر فرمت داده ها در فریم های اطلاعاتی با یکدیگر متفاوت می باشند.

تکنولوژی های متفاوت شبکه

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

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

شبکه

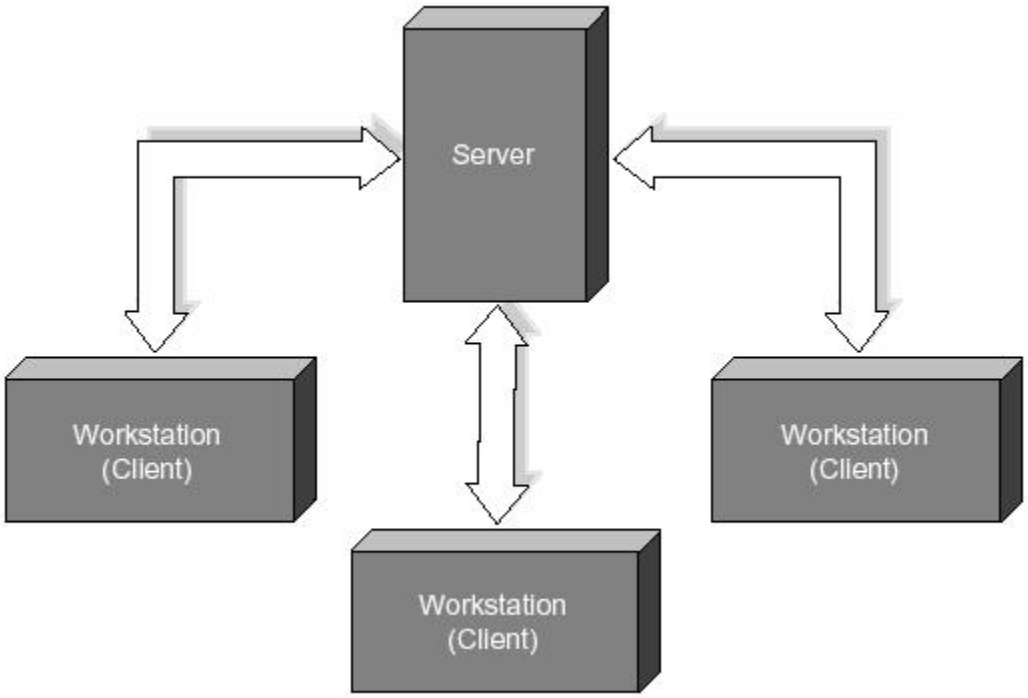
یک شبکه شامل مجموعه ای از دستگاهها (کامپیوتر ، چاپگر و ...) بوده که با استفاده از یک روش ارتباطی (کابل ، امواج رادیوئی ، ماهواره) و بمنظور اشتراک منابع فیزیکی (چاپگر) و اشتراک منابع منطقی (فایل) به یکدیگر متصل می گردند. شبکه ها می توانند با یکدیگر نیز مرتبط شده و شامل زیر شبکه هائی باشند.

تفسیم بندی شبکه ها

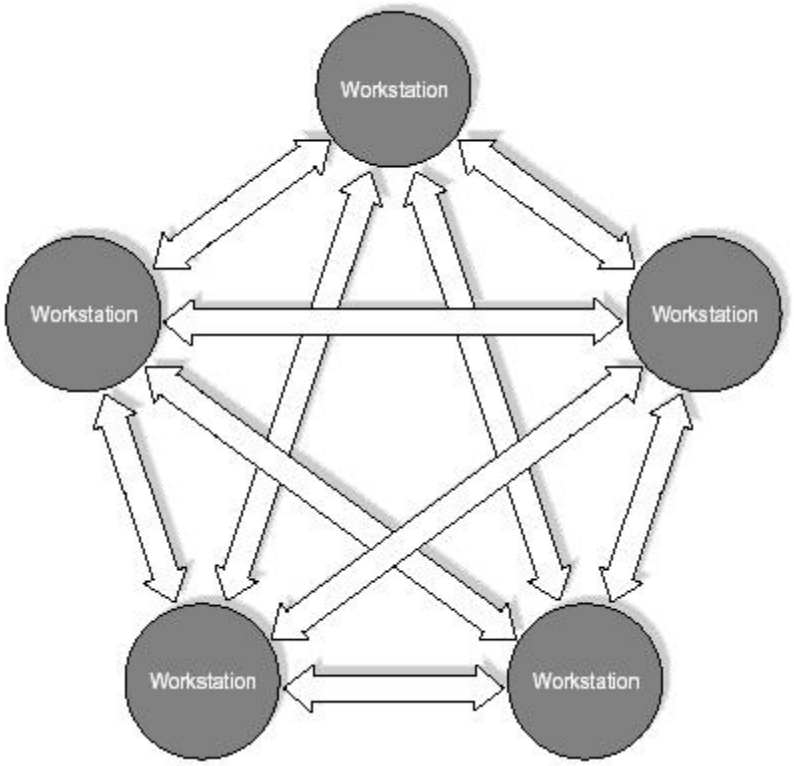
شبکه های کامپیوتری را بر اساس مولفه های متفاوتی تقسیم بندی می نمایند. در ادامه به برخی از متداولترین تقسیم بندی های موجود اشاره می گردد .

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

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



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



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

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

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

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

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

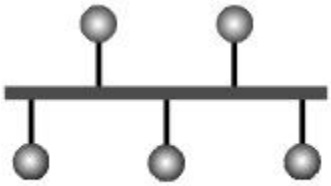
تصرف و بکارگیری ساختمان انجام گرفته باشد. بهرحال می بایست هزینه نصب شبکه بهینه گردد.

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

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

- BUS
- STAR
- RING

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



Bus

مزایای توپولوژی BUS

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

-*ساختار ساده* . توپولوژی BUS دارای یک ساختار ساده است . در مدل فوق صرفا" از یک کابل برای انتقال اطلاعات استفاده می شود.

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

معایب توپولوژی BUS

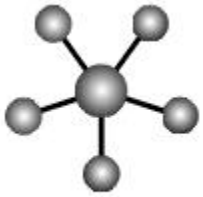
-*مشکل بودن عیب یابی* . با اینکه سادگی موجود در تویولوژی BUS امکان بروز اشتباه را کاهش می دهند، ولی در صورت بروز خطاء کشف آن ساده نخواهد بود. در شبکه هائی که از توپولوژی فوق استفاده می نمایند ، کنترل شبکه در هر گره دارای مرکزیت نبوده و در صورت بروز خطاء می بایست نقاط زیادی بمنظور تشخیص خطاء بازدید و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

-*ایزوله کردن خطاء مشکل است* . در صورتیکه یک کامپیوتر در توپولوژی فوق دچار مشکل گردد ، می بایست کامپیوتر را در محلی که به شبکه متصل است رفع عیب نمود. در موارد خاص می توان یک گره را از شبکه جدا

کرد. در حالتیکه اشکال در محیط انتقال باشد ، تمام یک سگمنت می بایست از شبکه خارج گردد.

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

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



Star

مزایای توپولوژی STAR

- *سادگی سرویس شبکه* . توپولوژی STAR شامل تعدادی از نقاط اتصالی در یک نقطه مرکزی است . ویژگی فوق تغییر در ساختار و سرویس شبکه را آسان می نماید.

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

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

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

معایب توپولوژی STAR

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

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

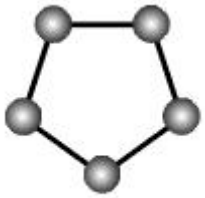
- *وابستگی به نقطه مرکزی* . در صورتیکه نقطه مرکزی (هاب) در شبکه با مشکل مواجه شود ، تمام شبکه

غیرقابل استفاده خواهد بود.

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

مزایای توپولوژی RING

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



Ring

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

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

معایب توپولوژی RING

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

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

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

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

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

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

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

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

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

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

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

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

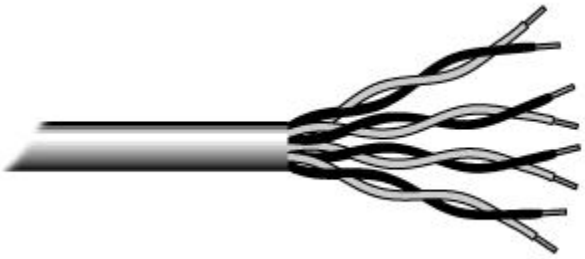
● کابل در شبکه

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

- کابل Unshielded Twisted pair)**UTP**)

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

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



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

Type	کاربرد
Cat 1	فقط صوت (کابل های تلفن)
Cat 2	داده با سرعت ٤ مگابیت در ثانیه
Cat 3	داده با سرعت ١٠ مگابیت در ثانیه
Cat 4	داده با سرعت ٢٠ مگابیت در ثانیه
Cat 5	داده با سرعت ١٠٠ مگابیت در ثانیه

مزایای کابل های بهم تابیده :

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

معایب کابل های بهم تابیده :

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

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

- کابل کواکسیال

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

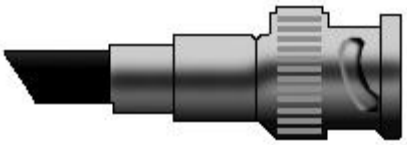
مزایای کابل های کواکسیال :

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

معایب کابل های کواکسیال :

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

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



- فیبر نوری

یکی از جدیدترین محیط های انتقال در شبکه های کامپیوتری ، فیبر نوری است . فیبر نوری از یک میله استوانه ای که هسته نامیده می شود و جنس آن از سیلیکات است تشکیل می گردد. شعاع استوانه بین دو تا سه میکرون است . روی هسته ، استوانه دیگری (از همان جنس هسته) که غلاف نامیده می شود ، استقرار می یابد. ضریب شکست هسته را با M1 و ضریب شکست غلاف را با M2 نشان داده و همواره M2<M1 است . در این نوع فیبرها ، نور در اثر انعکاسات کلی در فصل مشترک هسته و غلاف ، انتشار پیدا خواهد کرد. منابع نوری در این نوع کابل ها ، دیود لیزری و یا دیودهای ساطع کننده نور می باشند.منابع فوق ، سیگنال های الکتریکی را به نور تبدیل می نمایند.

مزایای فیبر نوری :

- حجم و وزن کم
- پهنای باند بالا
- تلفات سیگنال کم و در نتیجه فاصله تقویت کننده ها زیاد می گردد.
- فراوانی مواد تشکیل دهنده آنها
- مصون بودن از اثرات القاهای الکترو معناطیسی مدارات دیگر
- آتش زا نبودن آنها بدلیل عدم وجود پالس الکتریکی در آنها
- مصون بودن در مقابل عوامل جوی و رطوبت
- سهولت در امر کابل کشی و نصب
- استفاده در شبکه های مخابراتی آنالوگ و دیجیتال
- مصونیت در مقابل پارازیت

معایب فیبر نوری :

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

کابل های استفاده شده در شبکه های اترنت

Maximum length	Cable Type	Specification
100 meters	Unshielded Twisted Pair	**10BaseT**
185 meters	Thin Coaxial	**10Base2**
500 meters	Thick Coaxial	**10Base5**
2000 meters	Fiber Optic	**10BaseF**
100 meters	Unshielded Twisted Pair	**100BaseT**
220 meters	Unshielded Twisted Pair	**100BaseTX**

TCP/IP

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

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

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

اجزای پروتکل TCP/IP

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

پروتکل های موجود در لایه Network پروتکل TCP/IP

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

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

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

پروتکل های موجود در لایه Application پروتکل TCP/IP

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

پروتکل ها خواهیم پرداخت .

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

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

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

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

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

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

مدل آدرس دهی IP

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

نحوه اختصاص IP

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

Subnetting

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

کالبد شکافی آدرس های IP

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

216.27.61.137

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

- 11011000.00011011.00111101.10001001

همانگونه که مشاهده می گردد ، هر IP از ۳۲ بیت تشکیل می گردد. بدین ترتیب می توان حداکثر ٤,٢٩٤,٩٦٧,٢٩٦ آدرس منحصر بفرد را استفاده کرد($٢^{٣٢}$) . مثلا" آدرس ٢٥٥,٢٥٥,٢٥٥,٢٥٥ 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 ٠,٠,٠,٠ ، 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 ١ تا ١٢٦ 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 ١٢٦ و هر یک از شبکه های فوق می توانند ١٦,٧٧٧,٢١٤ کامپیوتر میزبان داشته باشند. (عدد فوق از طریق حاصل ٢ - $٢^{٢٤}$ بدست آمده است) بنابراین تعداد تمام کامپیوترهای میزبان در شبکه های کلاس A معادل ٢,١٤٧,٤٨٣,٦٤٨ ($٢^{٣١}$) است . در شبکه های کلاس A ، بیت با ارزش بالا در اولین octet همواره مقدار صفر را دارد.

Host (Node)	NET
24.53.107	**115.**

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 ($۲^{۳۰}$) است در شبکه های کلاس B ، اولین و دومین بیت در اولین octet به ترتیب مقدار یک و صفر را دارا می باشند.

Host (Node)	NET
53.107	145.24.

- **کلاس C** . کلاس فوق برای شبکه های کوچک تا متوسط در 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 ($۲^{۲۹}$) است . در شبکه های کلاس C ، اولین ، دومین و سومین بیت در اولین octet به ترتیب مقدار یک ، یک و صفر را دارا می باشند.

Host(Node)	NET
107	195.24.53.

- **کلاس D** . از کلاس فوق برای multicasts استفاده می شود. در چنین حالتی یک گره (میزبان) بسته اطلاعاتی خود را برای یک گروه خاص ارسال می دارد. تمام دستگاه های موجود در گروه ، بسته اطلاعاتی ارسال شده را دریافت خواهند کرد. (مثلا" یک روتر سیسکو آخرین وضعیت بهنگام شده خود را برای سایر روترهای سیسکو ارسال می دارد) کلاس فوق نسبت به سه کلاس قبلی دارای ساختاری کاملا" متفاوت است. اولین ، دومین ، سومین و چهارمین بیت به ترتیب دارای مقادیر یک ، یک ، یک و صفر می باشند.۲۸ بیت باقیمانده 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 ($۲^{۲۶}$) کامپیوتر است

Host(Node)	NET
24.53.107	224.

- **کلاس E** . از کلاس فوق برای موارد تجربی استفاده می شود. کلاس فوق نسبت به سه کلاس اولیه دارای ساختاری متفاوت است . اولین ، دومین ، سومین و چهارمین بیت به ترتیب دارای مقادیر یک ، یک ، یک و یک می باشند.۲۸ بیت باقیمانده 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 ($۲^{۲۶}$) کامپیوتر است

Host(Node)	NET
24.53.107	240.

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

255.255.255.255.

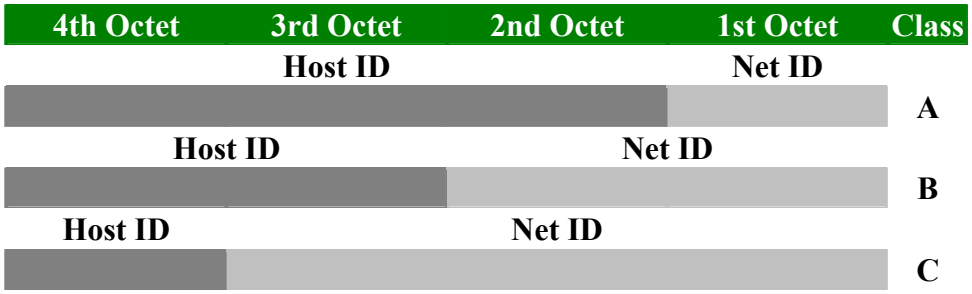
- **آدرس های رزو شده** . آدرس های IP زیر بمنظور استفاده در شبکه های خصوصی (اینترانت) رزو شده اند :

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

- **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. :

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

خلاصه :

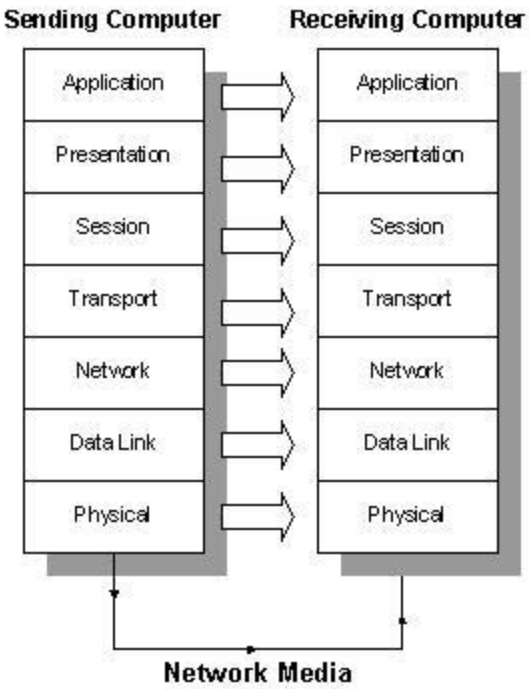


Comments	Normal Netmask	Address Range	Network Type
For very large networks	255.0.0.0	001.x.x.x to 126.x.x.x	Class A
For medium size networks	255.255.0.0	128.1.x.x to 191.254.x.x	Class B
For small networks	255.255.255.0	192.0.1.x to 223.255.254.x	Class C
Used to support multicasting		224.x.x.x to 239.255.255.255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

OSI

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

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



لایه های OSI

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

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

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

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

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

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

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

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

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

پروتکل های پشته ای

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

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

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

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

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

شبکه های بدون کابل

شبکه های بدون کابل یکی از چندین روش موجود بمنظور اتصال چند کامپیوتر بیکدیگر و ایجاد یک شبکه کامپیوتری است . در شبکه های فوق برای ارسال اطلاعات بین کامپیوترهای موجود در شبکه از امواج رادیوئی استفاده می شود.

مبانی شبکه های بدون کابل

تکنولوژی شبکه های بدون کابل از ایده **" ضرورتی به کابل ها ی جدید نمی باشد"** ، استفاده می نمایند. در این نوع شبکه ها ، تمام کامپیوترها با استفاده از سیگنال هائی رادیوئی اقدام به انتشار اطلاعات مورد نظر برای یکدیگر می نمایند. این نوع شبکه ها دارای ساختاری ساده بوده و براحتی می توان یک کامپیوتر متصل به این نوع از شبکه ها را مکان های دیگر استقرار و کماکن از امکانات شبکه بهره مند گردید مثلا" در 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 802.11 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 :

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

دو روش فوق از تکنولوژی Frequency-shift keying(FSK) استفاده می نمایند. همچنین دو روش فوق از امواج رادیوئی Spread-spectrum در محدوده ٤/ ٢ 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" ٢٢ 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" ٤٠٠ میلی ثانیه) ، بنابراین می توان از جندین 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 protocol Shared Wireless Access(SWAP) را ایجاد نموده است . SWAP دارای شش کانال صوتی متفاوت بر اساس استاندارد DECT و ٨٠٢,١١ است.
دستگاههای SWAP در هر ثانیه ٥٠ 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 ١٢٧ 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 (٧٥ تا ١٢٥ فوت / ٢٣ تا ٣٨ 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 .

ترانسیور بدون کابل واقعی بهمراه یک آنتن کوچک در یک کارت ISA , PCI 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 مبتنی بر استاندارد IEEE 802.11 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 ۸۰۲,۱۱b ، 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 802.11 (اولیه) سازگار است .

برخی از اشکالات Wi-Fi عبارتند از :

- گران قیمت می باشند.
- پیکربندی و تنظیمات آن مشکل است .
- نوسانات سرعت زیاد است .

Wi-Fi سرعت شبکه های اترنت را بدون استفاده از کابل در اختیار قرار می دهد. کارت های سازگار با Wi-Fi 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.

اشتراک منابع

یکی از اهداف اولیه و مهم دربرپاسازی شبکه های کامپیوتری ،اشتراک منابع است . منابع موجود در کامپیوتر به دو گروه عمده منابع فیزیکی (چاپگر) و منابع منطقی (فایل ها) تقسیم می گردند. پس از ایجاد یک شبکه می توان با توجه به بستر ایجاد شده عملیات متفاوتی را انجام داد :

- اشتراک یک چاپگر بمنظور استفاده توسط کامپیوترهای موجود در شبکه
- استفاده از یک خط ارتباطی اینترنت توسط کامپیوترهای موجود در شبکه
- اشتراک فایل ها ی اطلاعاتی با محتویات متفاوت
- استفاده از بازیهای کامپیوتری که چندین کاربر بصورت همزمان می توانند از آن استفاده نمایند.
- ارسال خروجی دستگاههائی نظیر دوربین های وب برای سایر کامپیوترهای موجود درشبکه

بمنظور بر پا سازی یک شبکه کامپیوتری کوچک، می بایست مراحل زیر را انجام داد :

- **انتخاب تکنولوژی مورد نظر جهت استفاده در شبکه** . اترنت بعنوان مهمترین تکنولوژی در این راستا مطرح است .

- **تهیه و نصب سخت افزارهای مربوطه**. هر یک از کامپیوترهای موجود در شبکه می بایست دارای یک کارت شبکه باشند.در صورت استفاده از توپولوژی ستاره (در حال حاضر متداولترین نوع توپولوژی است) می بایست از یکدستگاه هاب و در موارد حرفه ای تر از یک دستگاه سوئیچ استفاده کرد . پس از نصب و پیکربندی هر یک از کارت های شبکه در کامپیوترهای مورد نظر ، با استفاده از کابل های مربوطه (عموما" از کابل بهم تابیده Cat5 استفاده می گردد) هر یک از کامپیوترها به هاب و یا سوئیچ متصل می گردند.

- **پیکربندی سیستم بمنظور استفاده از منابع مشترک در سیستم**

این مرحله(پیکربندی سیستم)، یکی از مراحل مهم در زمینه آماده سازی شبکه برای استفاده توسط کاربران است .در این مرحله می بایست عملیات زیر صورت پذیرد :

- نامگذاری کامپیوتر
- اشتراک فایل ها
- اشتراک چاپگر
- امنیت
- اشتراک خط اینترنت

در ادامه به بررسی نحوه انجام هر یک از عملیات فوق خواهیم پرداخت .

نامگذاری کامپیوتر

قبل از اینکه کامپیوتری بعنوان یکی از گره های شبکه مطرح گردد ، می بایست برای آن نام و یک گروه را مشخص کرد. هر یک از کامپیوترهای موجود در شبکه می بایست دارای یک نام منحصر بفرد و یک نام گروه یکسان باشند. برای مشخص نمودن نام کامپیوتر و گروه ، عملیات زیر را می بایست انجام داد.

مرحله اول : در کامپیوترهائی با سیستم عامل ویندوز ۹۸ و یا میلینیوم ، موس را برروی Network Neighborhood (موجود بر روی صفحه اصلی) قرارداده و کلید سمت راست موس را فعال نمائید.

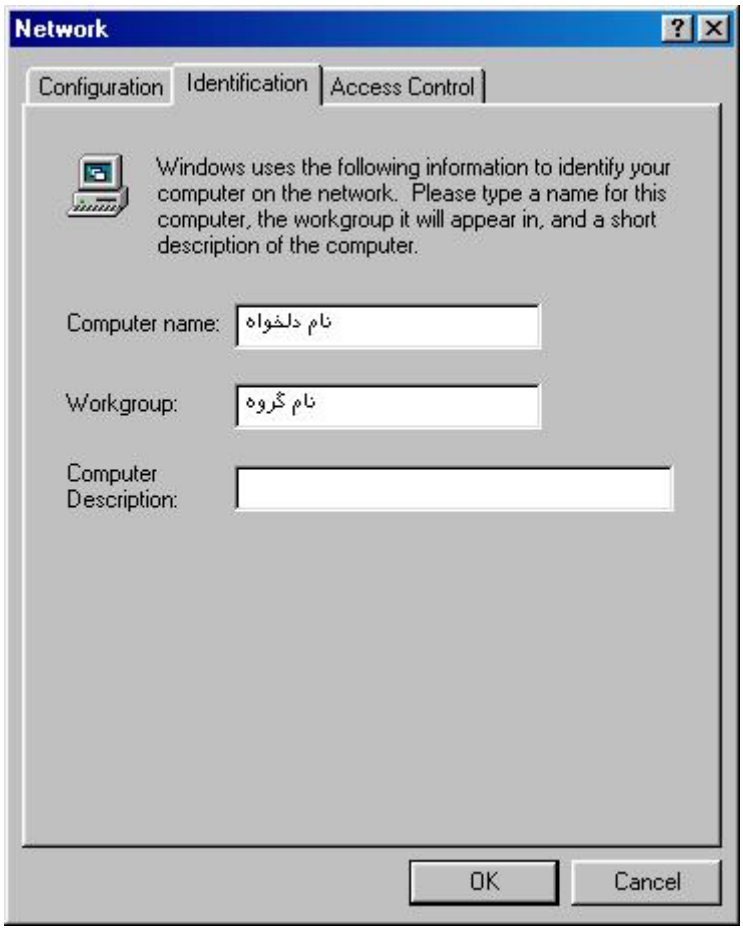
مرحله دوم : گزینه Properties را از طریق منوی دستورات انتخاب نمائید. در ادامه پنجره Network Properties فعال می گردد.در پنجره فوق اطلاعاتی در رابطه با آدپتورهای شبکه و پروتکل های نصب شده بر

روی کامپیوتر ، نمایش داده می شود.

مرحله سوم : پس از فعال شده پنجره اشاره شده ، گزینه Identification را انتخاب نمائید. در این حالت سه فیلد اطلاعاتی نمایش داده می شود.

مرحله چهارم : دراولین فیلد اطلاعاتی ، نام مورد نظر خود را برای کامپیوتر وارد نمائید. نام در نظر گرفته شده کاملا" انتخابی است و تنها محدودیت موجود ، تکراری نبودن آن است . سایر کامپیوترهای موجود در شبکه نباید از نام فوق استفاده کرده باشند.

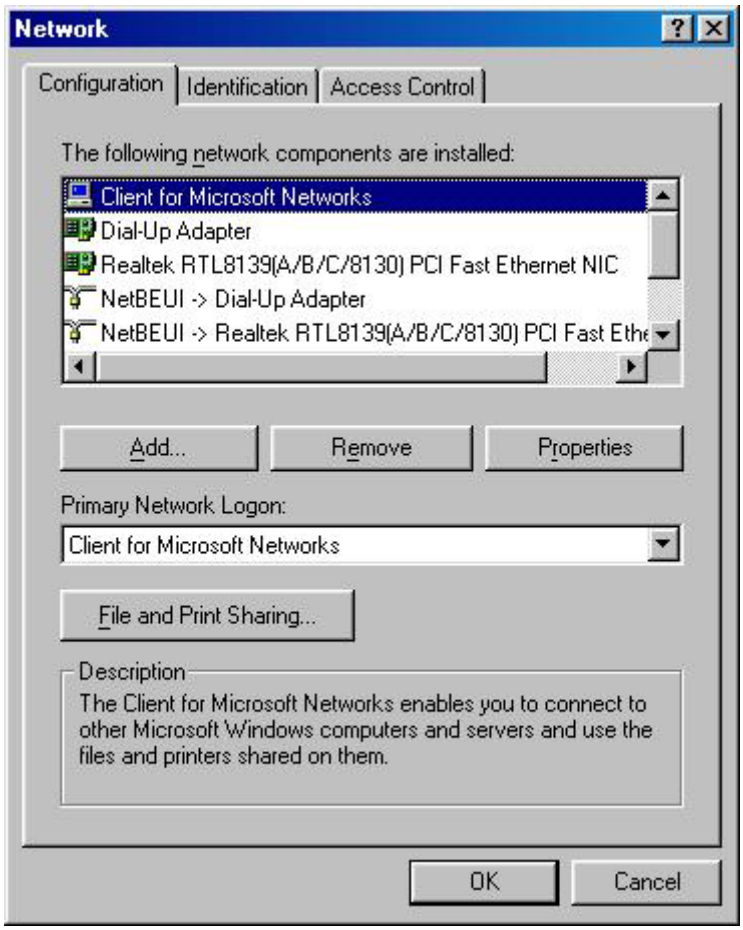
مرحله پنجم : دردومین فیلد اطلاعاتی ، نام در نظر گرفته شده برای گروه را وارد نمائید. تمام کامپیوترهای موجود در شبکه که قصد به اشتراک گذاشتن منابع سخت افزاری و نرم افزاری بین خود را دارند ، می بایست دارای نام گروه مشابه و یکسان باشند.



اشتراک فایل و امنیت

یکی از مهمترین عملیات در هر شبکه کامپیوتری ، اشتراک فایل ها است . در سیستم هائی که از ویندوز ۹۸ و یا میلینیوم استفاده می نمایند ، فرآیند فوق بسادگی انجام خواهد شد. پس از پیکربندی مناسب ، هر یک از کامپیوترهای موجود در شبکه قادر به اشتراک فایل بین خود خواهند بود. بمنظور فعال نمودن ویژگی فوق در ابتدا می بایست از فعال شدن گزینه File and Printer Sharing مطمئن گردید. بدین منظور موس را برروی امکان Network Neighborhood (موجود بر روی صفحه اصلی) قرارداده و کلید سمت راست موس را فعال

نمائید.گزینه Properties را از طریق منوی دستورات انتخاب نمائید. در ادامه پنجره Network Properties فعال می گردد . در ادامه گزینه Configuration فعال و در بخش پایین پنجره فوق ، امکان Client for Microsoft Networks می بایست مشاهده گردد. زمانیکه کامپیوتری بعنوان یک سرویس گیرنده (Client) در شبکه ای مطرح باشد ، قادر به تبادل اطلاعاتی با سایر کامپیوترهای موجود در شبکه خواهد بود. زمانیکه عملیات مربوط به پیکربندی و تنظیم شبکه در ویندوزهای ۹۸ و یا میلینیوم انجام می گیرد ، امکان اشاره شده بصورت اتوماتیک در سیستم اضافه خواهد گردید. در صورتیکه امکان فوق بصورت اتوماتیک اضافه نشده باشد ، می توان با دنبال نمودن مراحل زیر ، آن را نصب نمود.



مرحله اول : گزینه Add را از طریق پنجره Network Properties انتخاب نمائید

مرحله دوم : گزینه Client را از لیست بنمایش در آمده انتخاب نمائید.

مرحله سوم : با فعال کردن گزینه Add لیستی از شرکت ها و تولید کنندگان متفاوت را در پانل سمت چپ مشاهده می نمائید.

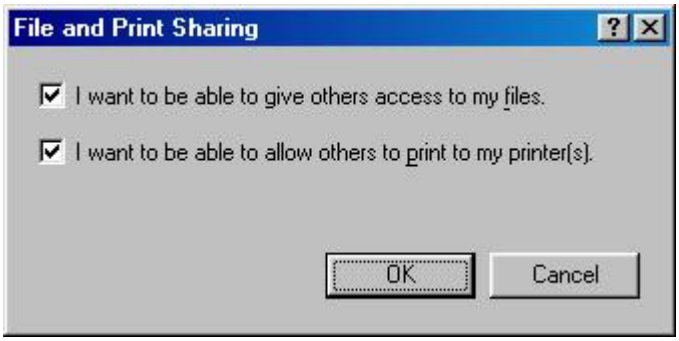
مرحله چهارم : گزینه Microsoft را از طریق پانل سمت چپ انتخاب و در ادامه لیستی از نرم افزارهای سرویس گیرنده مایکروسافت در پانل سمت راست نمایش داده خوواهند شد.

مرحله پنجم : از لیست فوق ، گزینه Microsoft Networks Client for را انتخاب و دکمه OK را فعال نمائید. در ادامه سیستم عامل ویندوز تمام فایل های ضروری و مورد نیاز را بر روی کامپیوتر قرار خواهد داد(

در این مرحله CD مربوط به ویندوز نیاز خواهد بود)

پس از نصب نرم افزارهای مورد نیاز ، می توان عملیات مربوط به اشتراک فایل ها را دنبال نمود. بدین منظور در پنجره اصلی (Network) شبکه مستقر شده و مراحل زیر را دنبال نمائید :

مرحله اول : دکمه مربوط به sharing File and print را فعال نمائید .



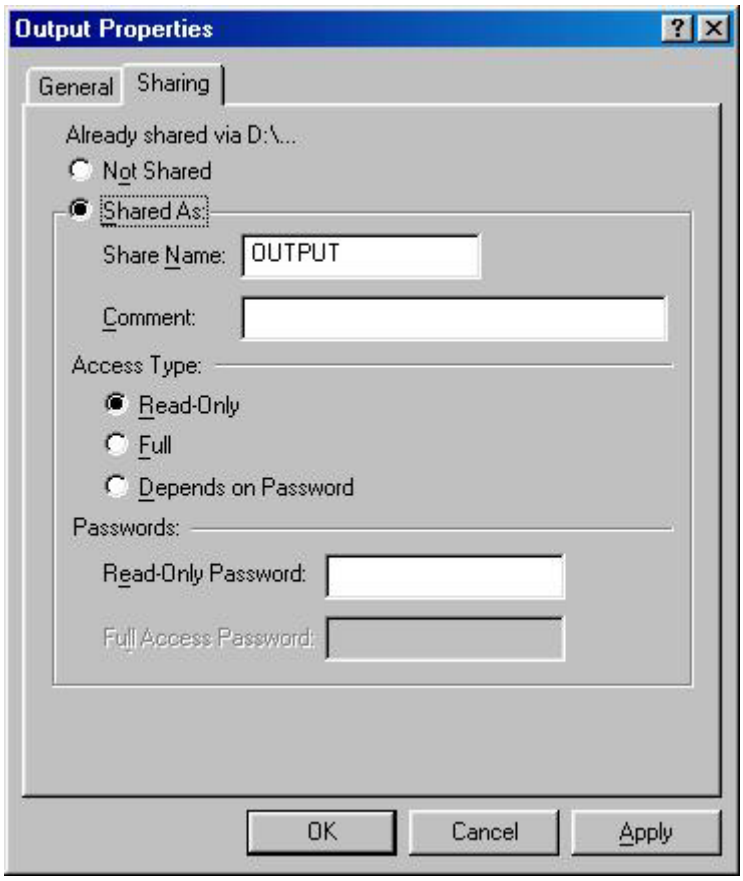
مرحله دوم : در این مرحله دو حق انتخاب وجود دارد. یکی برای اشتراک فایل ها و دیگری برای اشتراک چاپگر. با توجه به وضعیت موجود شبکه می توان یک و یا هر دو آیتم را انتخاب کرد.

مرحله سوم : پس از انتخاب هر یک از گزینه های مورد نظر (فایل ، چاپگر) ، یک Checkmark در کنار گزینهFile and print sharing فعال خواهد شد. با فعال نمودن دکمه OK پنجره مربوط به Sharing-options بسته خواهد شد.

مرحله چهارم : در ادامه امکان Control Access را از طریق پنجره Network انتخاب نمائید. بمنظور کنترل ساده در رابطه با هویت افرادیکی می توانند از فایل ها استفاده نمایند ، گزینه Share-level Access Control را انتخاب نمائید.

مرحله پنجم : با فعال کردن دکمه OK ، پنجره Network بسته خواهد شد.

در ادامه می بایست فولدرهائی را که قصد به اشتراک گذاشتن آنها را دارید ، مشخص نمائید. با ایجاد فولدرهای دلخواه و استقرار فایل های مورد نظر درهر یک می توان یک انظباط اطلاعاتی از بعد ذخیره سازی را ایجاد کرد. برای به اشتراک گذاشتن یک فولدر ، بر روی فولدر فوق مستقر و کلید سمت راست موس را فعال نمائید . گزینه Sharing را از طریق منوی مربوطه انتخاب نمائید. در ادامه پنجره ای فعال می گردد که در آن امکان انتخاب چندین آیتم وجود دارد. مقدار پیش فرض برای Sharing بصورت Not Shared است . با تغییر مقدار گزینه فوق و تبدیل آن به Shared As می توان در فیلد اطلاعاتی Share Name ، نام دلخواه خود را برای فولدر به اشتراک گذاشته شده مشخص نمود. نام فوق می تواند با نام واقعی فولدر کاملا" متفاوت می باشد. در صورتیکه قبلا" گزینه Access Control Share-level را انتخاب کرده باشید ، می بایست در ادامه سطح مورد نظر امنیتی (Access Type) را مشخص و برای آن یک رمز عبور را نیز مشخص نمود. دستیابی به روش Read-only بدین مفهوم است که هر کاربر قادر به دستیابی به فولدر از طریق شبکه بوده و صرفا" قادر به مشاهده و بازیابی فایل ها خواهد بود. این نوع کاربران قادر به استقرار فایل های جدید در فولدر و یا حذف و اصلاح فایل های موجود در فولدر نخواهند بود. در صورتیکه روش دستیابی به فولدر ، Full access تعیین گردد ، کاربران قادر به مشاهده ، نوشتن ، ایجاد و حذف فایل در فولدر مورد نظر خواهند بود. با توجه به نوع رمز عبور می توان هر دو گزینه را بصورت شناور نیز استفاده نمود.



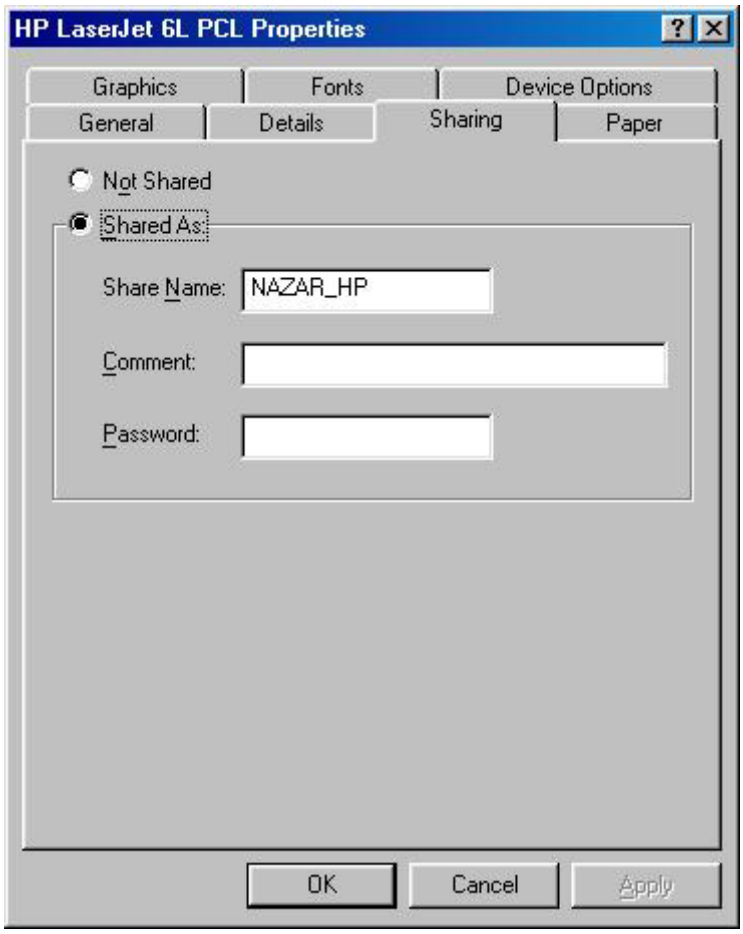
اشتراک چاپگر

بمنظور اشتراک یک چاپگر در ابتدا می بایست از صحت عملیات اشاره شده خصوصا" فعال شدن File and Printer Sharing اطمینان حاصل کرد. در ادامه با دنبال نمودن مراحل زیر می توان برای به اشتراک گذاشتن یک چاپگر مراحل زیر را دنبال نمود.

مرحله اول : از طریق دکمه Start ، گزینه Setting و در ادامه Printers را انتخاب نمائید.در ادامه پنجره ای شامل لیستی از تمام چاپگرهای محلی نمایش داده خواهد شد.

مرحله دوم : موس را بر روی آیکون چاپگری که قصد به اشتراک گذاشتن آن را دارید ، قرار داده و کلید سمت راست موس را فعال و گزینه Sharing را انتخاب نمائید.

مرحله سوم : در ادامه پنجره Properties فعال می گردد. در فیلد اطلاعاتی Shared As نام دلخواه برای چاپگر (بمنظور اشتراک گذاشتن) را مشخص نمائید. در صورت تمایل یک رمز عبور نیز را در این مرحله مشخص نمود.



مرحله چهارم : با فعال کردن دکمه OK ، پنجره مربوطه بسته شده و چاپگر به اشتراک گذاشته شده است .

بمنظور دستیابی به چاپگر به اشتراک گذاشته شده از طریق کامپیوترهای دیگر ، مراحل زیر را دنبال نمائید:

مرحله اول : پنجره مربوط به Printer را فعال نمائید.

مرحله دوم : ویزارد(برنامه کمکی) Printer Add a را فعال نمائید.

مرحله سوم : گزینه Network Printer را انتخاب و دکمه OK را فعال نمائید.

مرحله چهارم : ویزارد مربوطه در ادامه لیستی از چاپگرهای به اشتراک گذاشته شده موجود بر روی شبکه را نمایش خواهد داد. در ادامه چاپگر مورد نظر را انتخاب و دکمه Next را فعال نمائید. در نهایت ویزارد مربوطه درایور مورد نظر را نصب خواهد کرد. (در برخی حالات ممکن است نیاز به CD و یا دیسکت حاوی درایور چاپگر وجود داشته باشد)

اشتراک خط اینترنت

با توجه به رشد شبکه ها ی کوچک ، شرکت مایکروسافت از نسخه ویندوز CE۹۸ به بعد امکانی با نام (Internet Connection Sharing(ICS را اضافه نموده است .با استفاده از ICS می توان یک کامپیوتر را که با استفاده از یکی از روش های رایج نظیر : مودم ، DSL ، ISDN و یا کابل به اینترنت متصل است ، به

اشتراک گذاشت . ویندوز CE۹۸ و سایر نسخه های ویندوز دارای یک ویزارد بمنظور فعال کردن امکان فوق می باشند. عناصر نرم افزاری مورد نیاز ICS بصورت پیش فرض بر روی کامپیوتر نصب نمی گردند. توجه داشته باشید که امکان فوق صرفا" می بایست بر روی کامپیوتری که به اینترنت متصل است ، فعال گردد. برای فعال نمودن امکان فوق(بر روی کامپیوترهائی که از نسخه ویندوز CE۹۸ استفاده می نمایند) می بایست مراحل زیر را دنبال کرد :

مرحله اول : از طریق Control Panel ، گزینهAdd/Remove Programs را انتخاب نمائید.

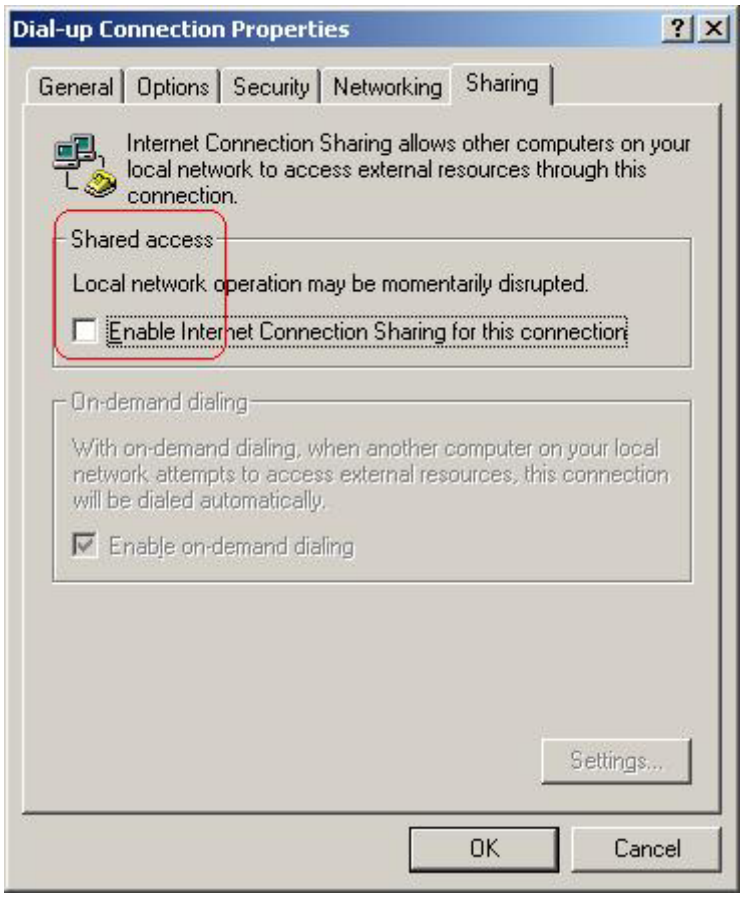
مرحله دوم : گزینه windows setup را انتخاب و در ادامه آیتم Internet Tools را انتخاب نمائید.

مرحله سوم : عنصر Sharing Internet Connection را انتخاب نمائید. در ادامه کلید Next را فعال نمائید. در صورتیکه ICS پیکربندی نشده باشد ، برنامه کمکی (ویزارد) مربوط به ICS فعال و در ادامه می توان عملیات پیکربندی لازم را انجام داد.

مرحله چهارم : پس از اخذ اطلاعات ضروری در رابطه با کامپیوتری که ICS بر روی آن فعال شده است ، ویزارد مربوطه نیاز به یک عدد دیسکت خواهد داشت . از اطلاعات ذخیره شده بر روی دیسکت فوق بمنظور پیکربندی سایر کامپیوترهای موجود در شبکه که تمایل به استفاده از سرویس ICS را داشته باشند استفاده می گردد.

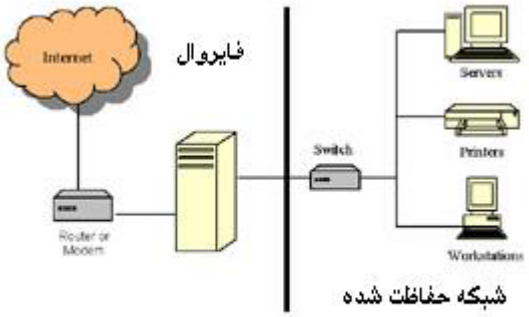
مراحل فعال نمودن سرویس ICS در کامپیوترهائی که از ویندوز ۲۰۰۰ و یا XP استفاده می نمایند بمراتب راحت تر از مراحل گفته شده فوق است .در این راستا پس از ایجاد یک Dial-up ، با انتخاب آن و فعال کردن کلید سمت راست ، گزینه Properties را انتخاب نمائید. در ادامه پنجره Dial-up Connection properties نمایش داده می شود.

برای اشتراک خطی ارتباط گزینه "Sharing" را انتخاب نمائید. در ادامه گزینه " Enable internet this connection connection sharing for" را انتخاب و سایر موارد و عملیات مورد نیاز بصورت اتوماتیک انجام خواهد شد.


Dial-up Connection Properties
General
Options
Security
Networking
Sharing
Internet Connection Sharing allows other computers on your local network to access external resources through this connection.
Shared access
Local network operation may be momentarily disrupted.
Enable Internet Connection Sharing for this connection
On-demand dialing
With on-demand dialing, when another computer on your local network attempts to access external resources, this connection will be dialed automatically.
Enable on-demand dialing
Settings...
OK
Cancel

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.



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 (T۱ و یا T3) 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 :

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

سوئیچ

شبکه از مجموعه ای کامپیوتر (گره) که توسط یک محیط انتقال (کابلی بدون کابل) بیکدیگر متصل می گردند ، تشکیل شده است. در شبکه از تجهیزات خاصی نظیر هاب و روتر نیز استفاده می گردد. سوئیچ یکی از عناصر اصلی و مهم در شبکه های کامپیوتری است . با استفاده از سوئیچ ، چندین کاربرقادربه ارسال اطلاعات از طریق شبکه در یک لحظه خواهند بود. سرعت ارسال اطلاعات هر یک از کاربران بر سرعت دستیابی سایر کاربران شبکه تاثیر نخواهد گذاشت . سوئیچ همانند روتر که امکان ارتباط بین چندین شبکه را فراهم می نماید ، امکان ارتباط گره های متفاوت (معمولا" کامپیوتر) یک شبکه را مستقیما" با یکدیگر فراهم می نماید. شبکه ها و سوئیچ ها دارای انواع متفاوتی می باشند.. سوئیچ هائی که برای هر یک از اتصالات موجود در یک شبکه داخلی استفاده می گردند ، سوئیچ های LAN نامیده می شوند. این نوع سوئیچ ها مجموعه ای از ارتباطات شبکه را بین **صرفا" دو دستگاه** که قصد ارتباط با یکدیگر را دارند ، در زمان مورد نظر ایجاد می نماید.

مبانی شبکه

عناصر اصلی در یک شبکه کـrامپیوتری بشرح زیر می باشند:

- **شبکه** . شبکه شامل مجموعه ای از کامپیوترهای متصل شده (با یک روش خاص)، بمنظور تبادل اطلاعات است .
- **گره** . گره ، شامل هر چیزی که به شبکه متصل می گردد ، خواهد بود.(کامپیوتر ، چاپگر و ...)
- **سگمنت**. سگمنت یک بخش خاص از شبکه بوده که توسط یک سوئیچ ، روتر و یا Bridge از سایر بخش ها جدا شده است .
- **ستون فقرات** . کابل اصلی که تمام سگمنت ها به آن متصل می گردند. معمولا" ستون فقرات یک شبکه دارای سرعت بمراتب بیشتری نسبت به هر یک از سگمنت های شبکه است . مثلا" ممکن است نرخ انتقال اطلاعات ستون فقرات شبکه ۱۰۰ مگابیت در ثانیه بوده در صورتیکه نرخ انتقال اطلاعات هر سگمنت ۱۰ مگابیت در ثانیه باشد.
- **توپولوژی** . روشی که هر یک از گره ها به یکدیگر متصل می گردند را گویند.
- **کارت شبکه** . هر کامپیوتر از طریق یک کارت شبکه به شبکه متصل می گردد.در اکثر کامپیوترهای شخصی ، کارت فوق از نوع اترنت بوده (دارای سرعت ۱۰ و یا ۱۰۰ مگابیت در ثانیه) و در یکی از اسلات های موجود روی برد اصلی سیستم ، نصب خواهد شد.
- **آدرس MAC** . آدرس فیزیکی هر دستگاه (کارت شبکه) در شبکه است. آدرس فوق یک عدد شش بایتی بوده که سه بایت اول آن مشخص کننده سازنده کارت شبکه و سه بایت دوم ، شماره سریال کارت شبکه است .
- **Unicast** . ارسال اطلاعات توسط یک گره با آدرس خاص و دریافت اطلاعات توسط گره دیگر است .
- **Multicast** . یک گره ، اطلاعاتی را برای یک گروه خاص (با آدرس مشخص) ارسال می دارد.دستگاههای موجود در گروه ، اطلاعات ارسالی را دریافت خواهند کرد.
- **Broadcast** . یک گره اطلاعاتی را برای تمام گره های موجود در شبکه ارسال می نماید.

استفاده از سوئیچ

در اکثر شبکه های متداول ، 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 فرآیند 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.

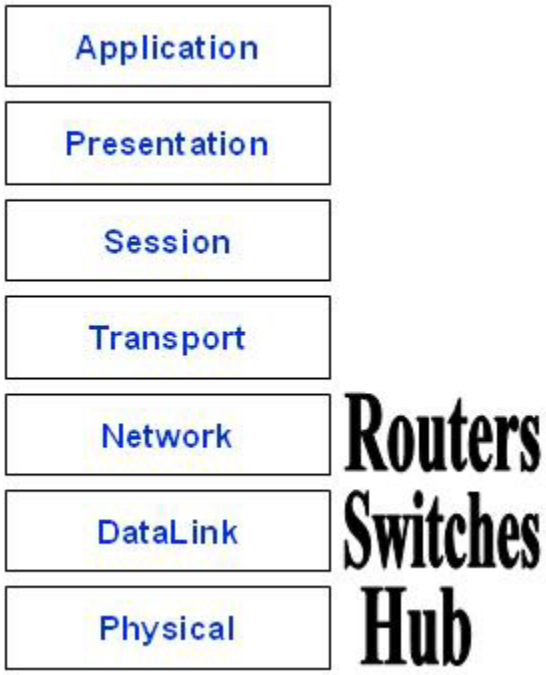
در شبکه های مبتنی بر سوئیچ امکان استفاده از کابل های بهم تابیده و یا فیبر نوری وجود خواهد داشت . هر یک از کابل های فوق دارای کانکتورهای مربوط به خود برای ارسال و دریافت اطلاعات می باشند. با استفاده از سوئیچ ، شبکه ای عاری از تصادم اطلاعاتی بوجود خواهد آمد. انتقال دو سویه اطلاعات در شبکه های مبتنی بر

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 .



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 ٦٤ بایت آن ذخیره می گردد.

سوئیچ های LAN دارای مدل های متفاوت از نقطه نظر طراحی فیزیکی می باشند. سه مدل رایج در حال حاضر بشرح زیر می باشند:

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

-Matrix . این نوع از سوئیچ ها دارای یک شبکه(تور) داخلی ماتریس مانند بوده که پورت های ورودی و خروجی همدیگر را قطع می نمایند. زمانیکه یک بسته اطلاعاتی بر روی پورت ورودی تشخیص داده شد

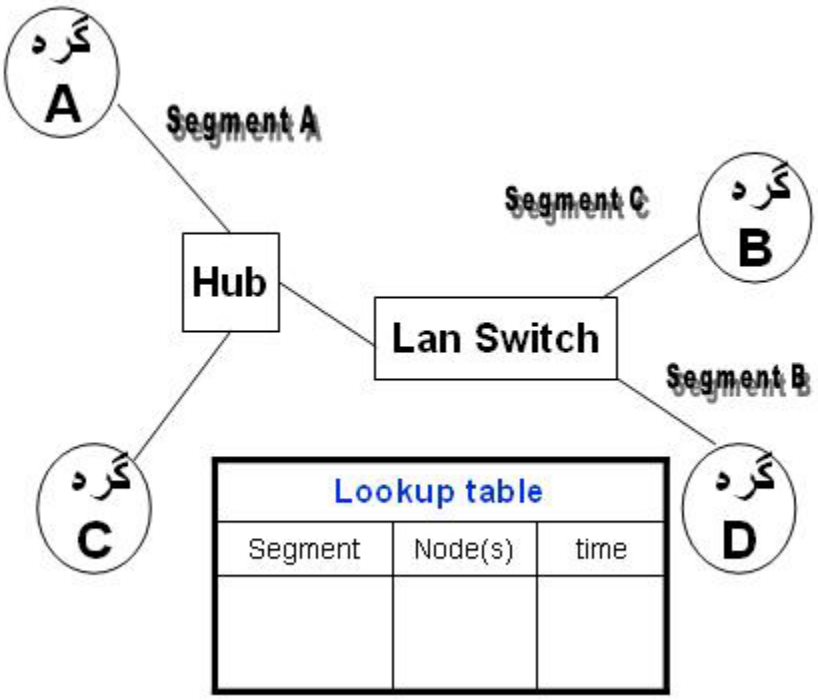
، آدرس MAC آن با جدول lookup مقایسه تا پورت مورد نظر خروجی آن مشخص گردد. در ادامه سوئیچ یک ارتباط را از طریق شبکه و در محلی که پورت ها همدیگر را قطع می کنند ، برقرار می گردد.

- 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



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.

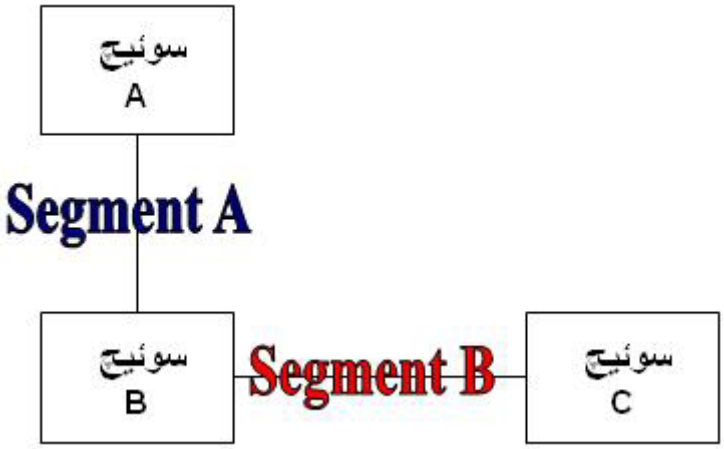
- گره C اطلاعاتی را از طریق سوئیچ برای گره A ارسال می دارد. سوئیچ آدرس MAC گره C را در جدول Lookup سگمنت A ذخیره می نماید ، سوئیچ آدرس گره A را دانسته و مشخص می گردد که دو گره A و C در یک سگمنت قرار دارند. بنابراین نیازی به ارتباط سگمنت A با سگمنت دیگر بمنظور ارسال اطلاعات گره C نخواهد بود. بدین ترتیب 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.

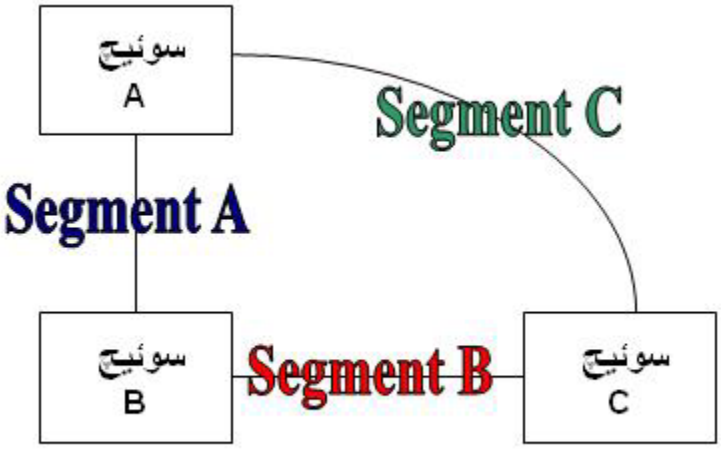
در مثال فوق ، دو گره سگمنت A را به اشتراک گذاشته و سگمنت های A و D بصورت مستقل می باشند. در شبکه های ایده آل مبتنی بر سوئیچ ، هر گره دارای سگمنت اختصاصی مربوط بخود است . بدین ترتیب امکان تصادم حذف و نیازی به عملیات Filtering نخواهد بود.

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 :



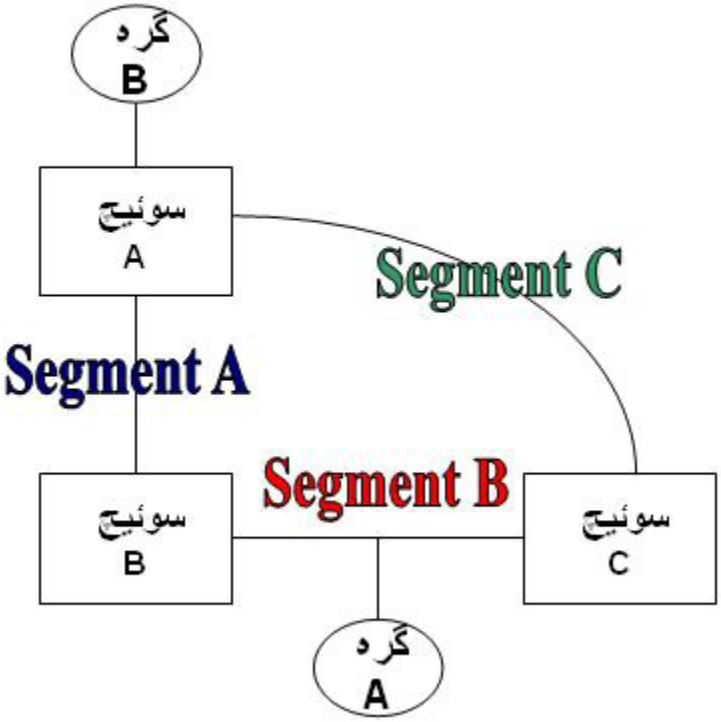
در مثال فوق ، در صورتیکه سوئیچ A و یا C با مشکل مواجه گردند، تمام گره های متصل به هر یک از سوئیچ های فوق نیز تحت تاثیر اشکال فوق قرار خواهند گرفت . گره های متصل به سوئیچ دیگر (B) کماکن قادر به ارائه خدمات خود خواهد بود. در صورتیکه سوئیچ C با اشکال مواجه گردد ، تمام شبکه از کار خواهد افتاد . در صورت اضافه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



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.



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 . Spanning tree 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 تقسیم 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
250	4 Mbps
100	10 Mbps
62	16 Mbps
39	45 Mbps
19	100 Mbps
14	155 Mbps
6	622 Mbps
4	1 Gbps
2	10 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 Bridge (BPUD 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 ارسال 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 .

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 switching Packet 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 ۹ base-T۱۰۰ ، 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 T1 یک نمونه متداول در این زمینه بوده و دارای سرعت ۱,۵ مگابیت در ثانیه است . برخی از موسسات با توجه به حساسیت و نوع کار خود می توانند از یک خط دیگر نیز بمنظور ارتباط روتر با ISP استفاده نمایند. خط فوق بصورت Backup بوده و بمحض بروز اشکال در خط اختصاصی (مثلا" T1) می توان از خط دوم استفاده نمود. با توجه به اینکه خط فوق بصورت موقت و در مواقع اضطراری استفاده می شود ، می توان یک خط با سرعت پایین 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 نمایید.

```
D:\>iPCONFIG/ALL

Windows 2000 IP Configuration

        Host Name . . . . . . . . . . . . : sakha-ravesh
        Primary DNS Suffix  . . . . . . . : sakharavesh.com
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : Yes
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : sakharavesh.com

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Realtek RTL8029(AS

        Physical Address. . . . . . . . . : 00-C0-DF-E8-3B-AB
        DHCP Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 10.10.1.7
        Subnet Mask . . . . . . . . . . . : 255.0.0.0
```

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 www.microsoft.com آگاهی پیدا نمائیم ، کافی است دستور فوق را بصورت زیر تایپ نمائیم :

Tracert www.microsoft.com

خروجی دستور فوق مشابه زیر است :

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

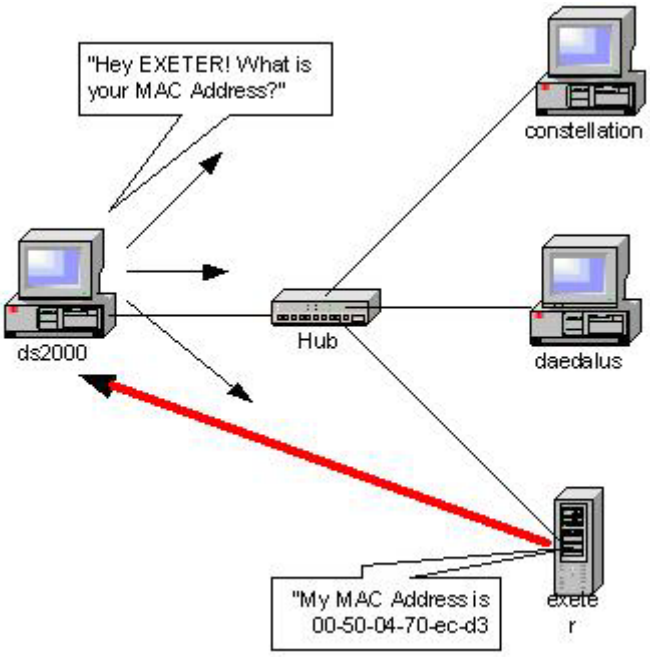
باتوجه به گستردگی اینترنت و وجود میلیون ها بسته اطلاعاتی در هر ثانیه بمنظور مسیریابی ، می بایست از روترهای با سرعت بالا استفاده شود. روتر سری ۱۲۰۰۰ سیسکو یکی از این نوع روترها بوده که بعنوان ستون فقرات اصلی در اینترنت استفاده می شود. تکنولوژی بکار گرفته شده در طراحی روترهای فوق مشابه سوپر کامپیوترها می باشد. (استفاده از پردازنده های با سرعت بالا بهمراه مجموعه ای از سوئیچ های پر سرعت). در روتر مدل ۱۲۰۰۰ از پردازنده های MHZ MIPS R5000۲۰۰ 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.

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 ds2000 قصد ارسال اطلاعات به کامپیوتری با نام Exeter را دارد. یک پیام Broadcast برای تمامی کامپیوترهای موجود در سگمنت ارسال خواهد شد. تمامی کامپیوترهای موجود در سگمنت مکلف به بررسی پیام می باشند. کامپیوتر Exeter پس از دریافت پیام ،آدرس MAC خود را برای کامپیوتر ds2000 ارسال می نماید.



همانگونه که اشاره گردید استفاده از پروتکل فوق برای برطرف مشکل اسامی (ترجمه نام یک کامپیوتر به آدرس فیزیکی و سخت افزاری) صرفا" برای شبکه های محلی با ابعاد کوچک توصیه شده و در شبکه های بزرگ نظیر شبکه های اترنت با ماهیت 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 بر NetBIOS (نظیر NetBEUI) دارای مکانیزمهای لازم برای روتینگ نبوده و دستورالعمل های مربوط به روتینگ در مشخصه فریم بسته های اطلاعاتی NetBIOS تعریف نشده است .
- در 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.

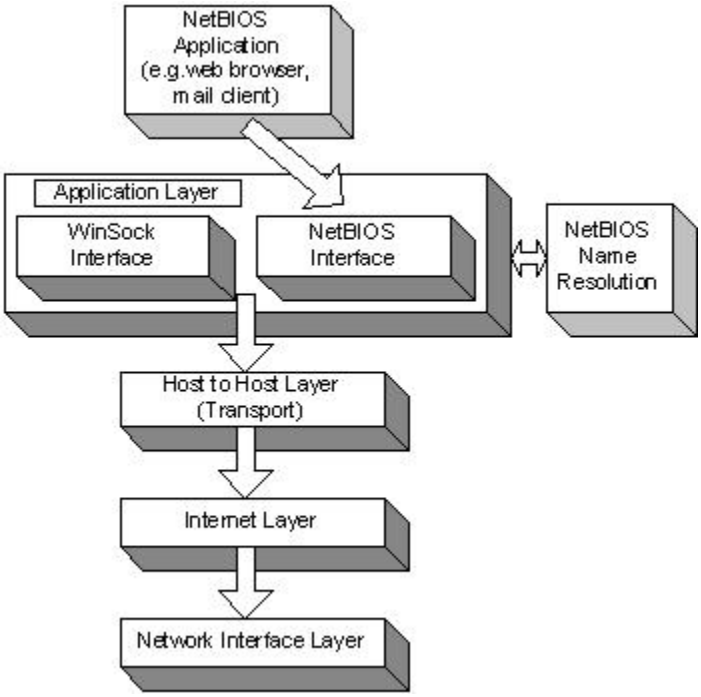
اینترفیس های NetBIOS و WinSock

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 گردند.

- 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.



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 Host Name نمی باشند می توان با رعایت تمامی مسائل جانبی از روش فوق برای ترجمه اسامی استفاده کرد. فرآیند فوق را ترجمه اسامی (Name Resoulation Host) می گویند.

موارد اختلاف بین NetBIOS و WinSock

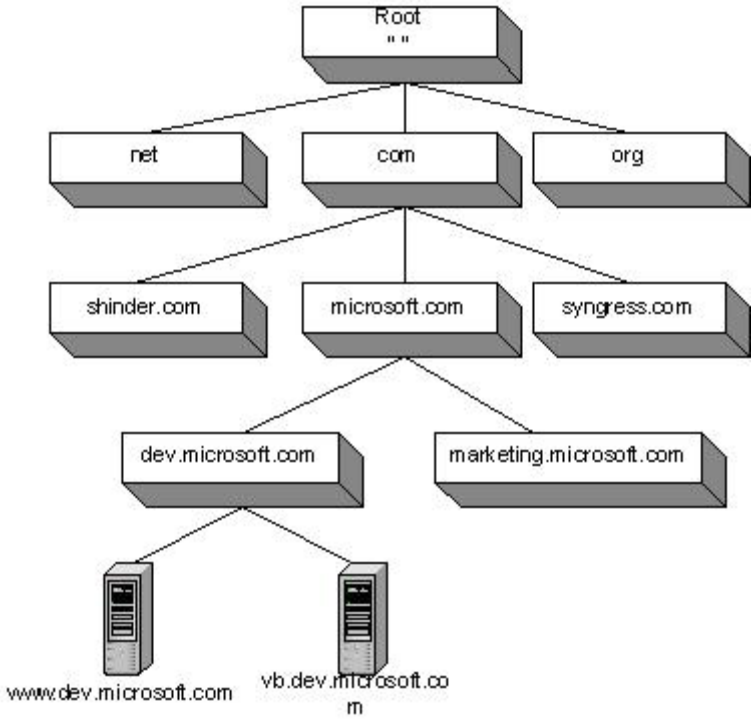
برنامه های مبتنی بر NetBIOS می بایست قبل از ایجاد ارتباط با یک کامپیوتر، نام NetBIOS را به یک IP ترجمه نمایند.(قبل از ایجاد ارتباط نام NetBIOS به IP تبدیل خواهد شد.) در برنامه های مبتنی بر WinSock

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.



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 Network Solutions Intcorporated(NSI) 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-8 استفاده می نماید. بر خلاف کاراکترهای اسکی که قبلا" از آنان استفاده می گردید. بهرحال FQDN می بایست دارای طولی به اندازه حداکثر ۲۵۵ بایت باشد.

طراحی نام حوزه برای یک سازمان

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

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

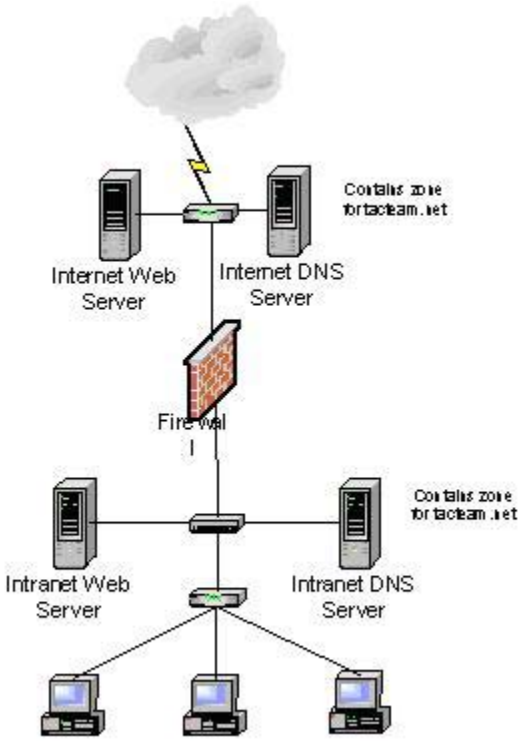
استفاده از نام یکسان دامنه برای منابع اینترنت و اینترانت

استفاده از اسامی یکسان برای نامگذاری دامنه 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

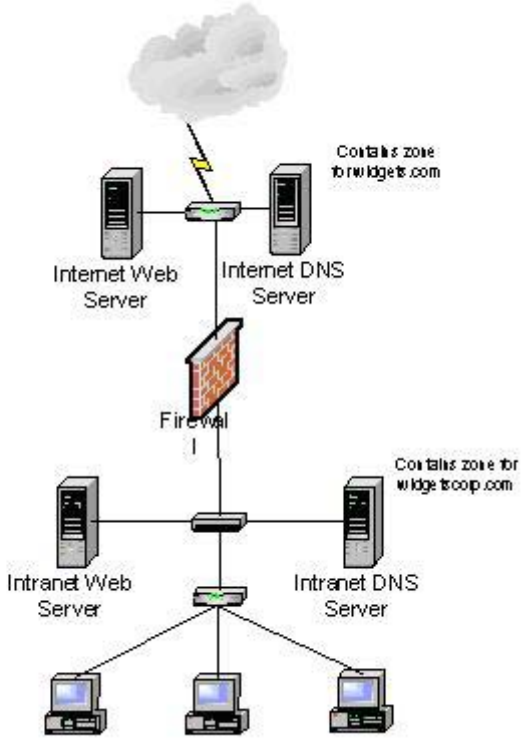
یکی دیگر از عملیاتی که می بایست در زمان پیاده سازی دامنه های یکسان برای منابع داخلی و خارجی مورد توجه قرار دارد Mirror نمودن منابع خارجی بصورت داخلی است . مثلا" فرض نمائید که Test.com نام انتخاب شده برای دستیابی به منابع داخلی (اینترانت) و منابع خارجی (اینترنت) است.درچنین وضعیتی دارای

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.



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 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%\system32\dns% خواهد بود. در این بخش هدف بررسی Zone های استاندارد بوده که به دو نوع عمده تقسیم خواهند شد.

- Forward Lookup Zone
- Reverse Lookup Zone

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

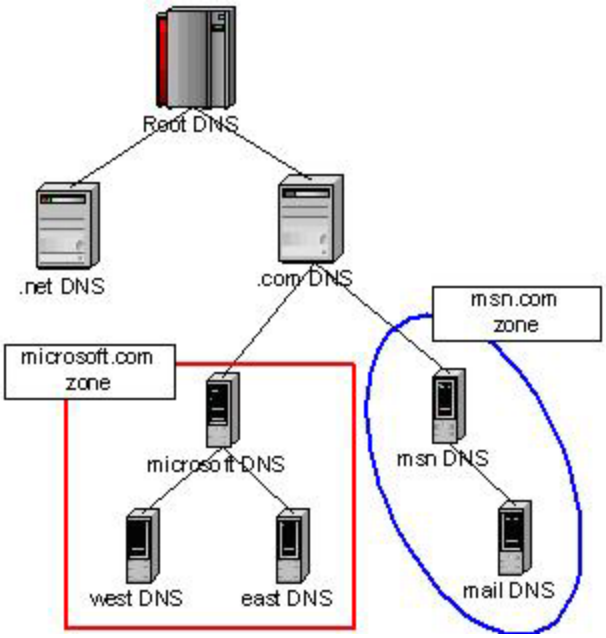
Lookup Zone Forward

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.

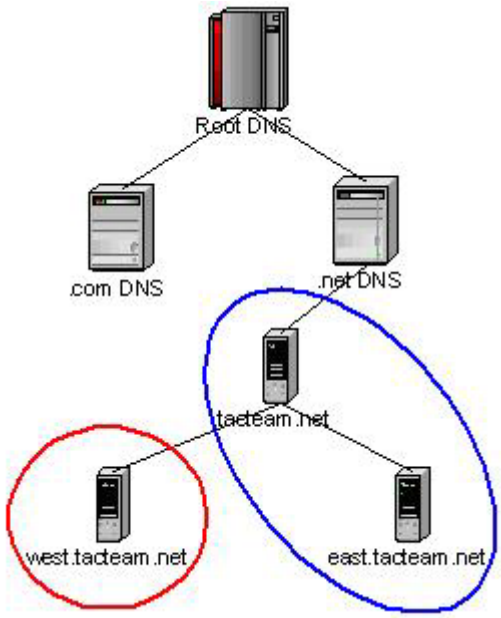
تفاوت بین Domain و Zone

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 West , East 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



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 گردند. 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 گردند؟ هر Zone نام خود را از طریق ریشه و یا بالاترین سطح دامنه اقتباس خواهند شد. زمانیکه درخواستی برای یک منبع موجود بر روی دامنه west.tacteam.net برای DNS واصل گردد (سرویس دهنده DNS مربوط به tacteam.net) سرویس دهنده tacteam.net صرفا" شامل یک Zone نخواهد بود.در چنین وضعیتی سرویس دهنده فوق دارای یک Delegation (واگذاری مسئولیت) بوده که به سرویس دهنده DNS مربوط به west.tacteam.net اشاره خواهد کرد. بنابراین درخواست مربوطه برای ترجمه اسامی به آدرس بدرستی به سرویس دهنده مربوطه هدایت تا مشکل برطرف گردد.



Reverse Lookup Zones

Zoneها ی از نوع Forward امکان ترجمه نام یک کامپیوتر به یک IP را فراهم می نمایند.یک Reverse Lookup این امکان را به سرویس گیرندگان خواهد داد که عملیات مخالف عملیات گفته شده را انجام دهند: ترجمه یک آدرس IP به یک نام . مثلا" فرض کنید شما می دانید که آدرس IP مربوط به کامپیوتر مقصد ۱۹۲,۱۶۸,۱,۳ است اما علاقه مند هستیم که نام آن را نیز داشته باشیم . 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 :

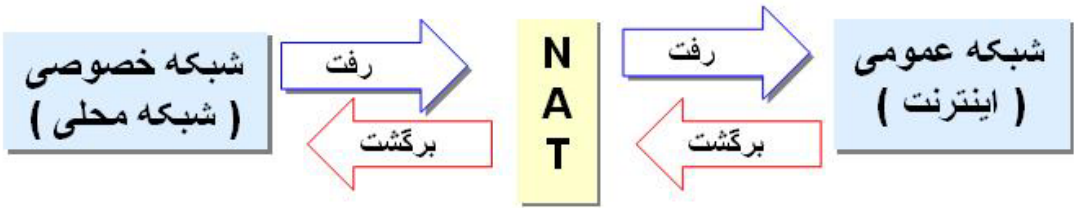
1.168.192.in-addr.arpa.dns

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 باAddress Network (Translation 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 شبکه را مشخص می کند.

اولین مرتبه ای که مسئله آدرس دهی توسط IP مطرح گردید، کمتر کسی به این فکر می افتاد که ممکن است خواسته ای مطرح شود که نتوان به آن یک آدرس را نسبت داد. با استفاده از سیستم آدرس دهی IP می توان ٤,٢٩٤,٩٧٦,٢٩٦ ($٢^{٣٢}$) آدرس را تولید کرد. (بصورت تئوری). تعداد واقعی آدرس های قابل استفاده کمتر از مقدار (بین ۳,۲ میلیارد و ۳,۳ میلیارد) فوق است . علت این امر، تفکیک آدرس ها به کلاس ها و رزو بودن برخی آدرس ها برای multicasting ، تست و موارد خاص دیگر است .

همزمان با انفجار اینترنت (عمومیت یافتن) و افزایش شبکه های کامپیوتری ، تعداد IP موجود، پاسخگوی نیازها نبود. منطقی ترین روش، طراحی مجدد سیستم آدرس دهی IP است تا امکان استفاده از آدرس های IP بیشتری 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.



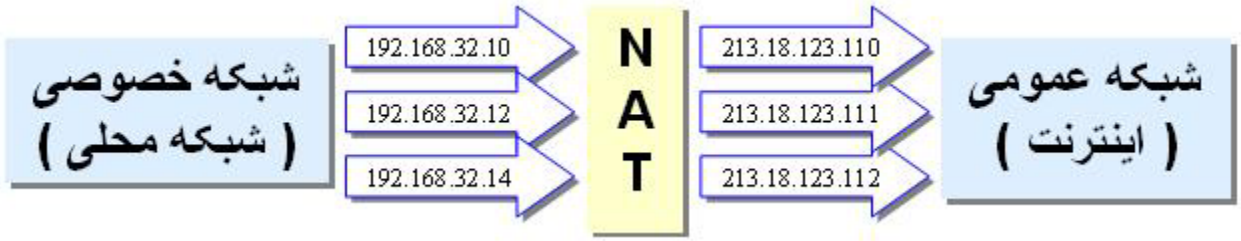
کم بودن تعداد IP صرفا" یکی از دلایل استفاده از NAT است .در ادامه به بررسی علل استفاده از NATخواهیم پرداخت .

قابلیت های NAT

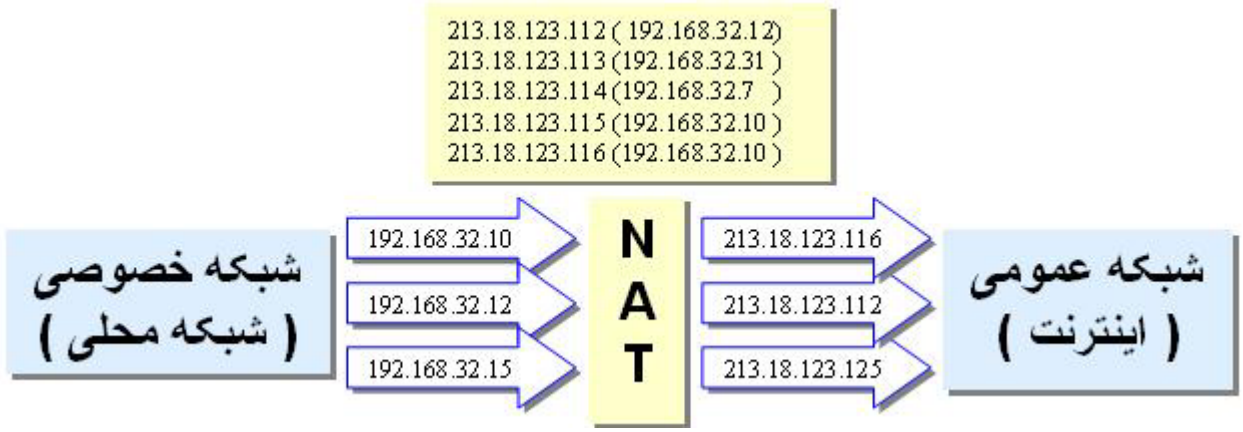
عملکرد NAT مشابه یک تلفنچی در یک اداره بزرگ است . فرض کنید شما به تلفنچی اداره خود اعلام نموده اید که تماس های تلفنی مربوط به شما را تا به وی اعلام ننموده اید ، وصل نکند . در ادامه با یکی ازمشتریان تماس گرفته و برای وی پیامی گذاشته اید که سریعا" با شما تماس بگیرد. شما به تلفنچی اداره می گوئید که منتظر 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 .

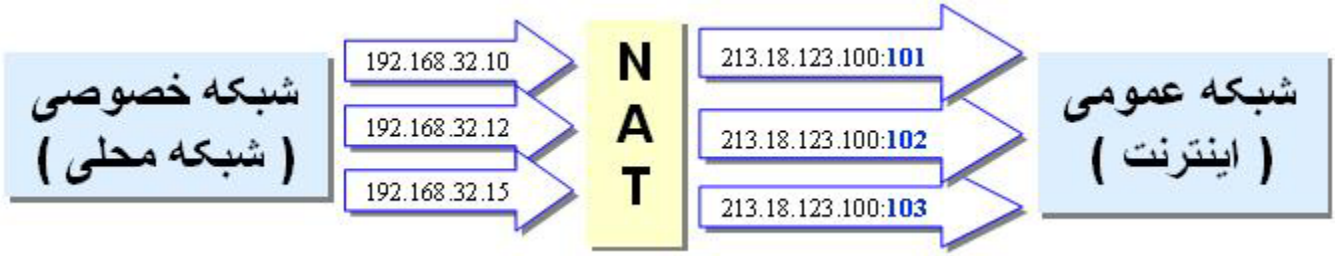
- **NAT ایستا** . عملیات مربوط به ترجمه یک آدرس IP غیر ریجستر شده (ثبت شده) به یک آدرس IP ریجستر شده را انجام می دهد. (تناظر یک به یک) روش فوق زمانیکه قصد استفاده از یک دستگاه را از طریق خارج از شبکه داشته باشیم، مفید و قابل استفاده است . در مدل فوق همواره 192.168.32.10 IP به IP ۲۱۳,۱۸,۱۲۳,۱۱۰ ترجمه خواهد شد.



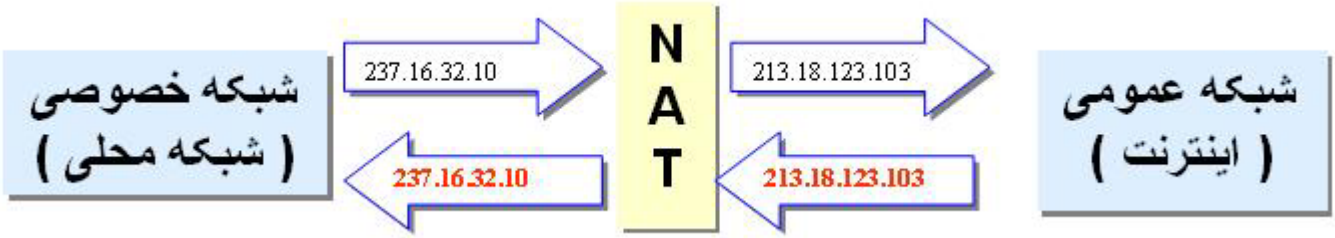
- **NAT پویا** . یک آدرس IP غیر ریجستر شده را به یک IP ریجستر شده ترجمه می نماید. در ترجمه فوق از گروهی آدرس های IP ریجستر شده استفاده خواهد شد.



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



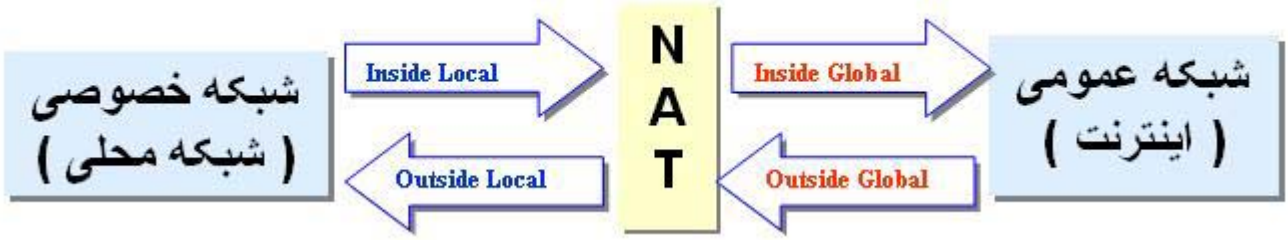
- **Overlapping** . در روش فوق شبکه خصوصی از مجموعه ای IP ریجستر شده استفاده می کند که توسط شبکه دیگر استفاده می گردند. NAT می بایست آدرس های فوق را به آدرس های IP ریجستر شده منحصربفرد ترجمه نماید. NAT همواره آدرس های یک شبکه خصوصی را به آدرس های ریجستر شده منحصر بفرد ترجمه می نماید. NAT همچنین آدرس های ریجستر شده عمومی را به آدرس های منحصر بفرد در یک شبکه خصوصی ترجمه می نماید. (در هر حالت خروجی NAT ، آدرس های IP منحصر بفرد خواهد بود. آدرس های فوق می تواند در شبکه های عمومی ریجستر شده جهانی باشند و در شبکه های خصوصی ریجستر شده محلی باشند)



شبکه اختصاصی (خصوصی) معمولا" بصورت یک شبکه LAN می باشند . به این نوع شبکه ها که از آدرس های IP داخلی استفاده می نمایند حوزه محلی می گویند. اغلب ترافیک شبکه در حوزه محلی بصورت داخلی بوده 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) که بر روی شبکه خصوصی (داخلی) می باشند را به آدرس های IP ریجستر شده ترجمه نماید.

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



- 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.(تعداد پورت های ممکن ٦٥٥٣٦ ($٢^{١٦}$) خواهد بود) . عملا" از تمام محدوده پورت های فوق استفاده نشده و ٤٠٠٠ پورت بصورت واقعی استفاده خواهند شد.

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 Assigned Numbers(IANA Authority) 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 Internet Assigned Numbers (IANA 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.

NAT Router's Assigned Port Number	NAT Router's IP Address	Source Computer's Port	Source Computer's IP Address	Source Computer
1	215.37.32.203	400	192.168.32.10	A
2	215.37.32.203	50	192.168.32.13	B
3	215.37.32.203	3750	192.168.32.15	C

4	215.37.32.203	206	192.168.32.18	D

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" ١٦٠ بایت را اشغال خواهد کرد، یک روتر با ٤ مگابایت حافظه قادر به پردازش ٢٦,٢١٤ 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 1: Class A - 10.0.0.0 through 10.255.255.255
Range 2: Class B - 172.16.0.0 through 172.31.255.255
Range 3: Class C - 192.168.0.0 through 192.168.255.255

امنیت

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.

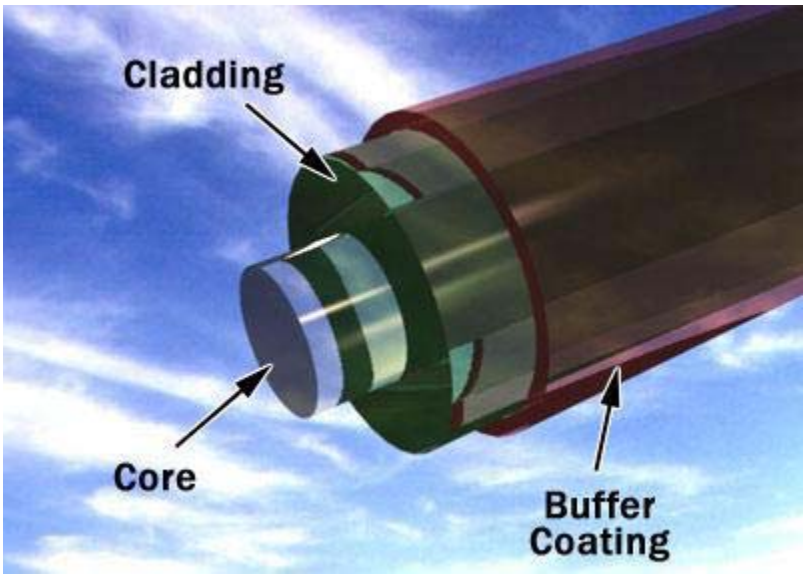
NAT دربرخی موارد با سرویس دهندگان Proxy ، اشتباه در نظر گرفته می شود. NAT و Proxy دارای تفاوت های زیادی می باشند. NAT بی واسطه بین کامپیوترهای مبداء و مقصد قرار می گیرد. Proxy بصورت بی واسطه نبوده و پس از استقرار بین کامپیوترهای مبداء و مقصد تصور هر یک از کامپیوترهای فوق را تغییر خواهد داد. کامپیوتر 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 .

فیبرنوری

فیبر نوری یکی از محیط های انتقال داده با سرعت بالا است . 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.

مبانی فیبر نوری

فیبر نوری ، رشته ای از تارهای بسیار نازک شیشه ای بوده که قطر هر یک از تارها نظیر قطر یک تار موی انسان است . تارهای فوق در کلاف هائی سازماندهی و کابل های نوری را بوجود می آورند. از فیبر نوری بمنظور ارسال سیگنال های نوری در مسافت های طولانی استفاده می شود.



یک فیبر نوری از سه بخش متفاوت تشکیل شده است :

- هسته (Core) . هسته نازک شیشه ای در مرکز فیبر که 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.

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)

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 .

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 .

بازیاب (تقویت کننده) نوری

همانگونه که قبلا" اشاره گردید ، برخی از سیگنال ها در مواردیکه مسافت ارسال اطلاعات طولانی بوده (بیش از یک کیلومتر) و یا از مواد خالص برای تهیه فیبر نوری (شیشه) استفاده نشده باشد ، تضعیف و از بین خواهند رفت . در چنین مواردی و بمنظور تقویت (بالا بردن) سیگنا ل های نوری تضعیف شده از یک یا چندین " تقویت کننده نوری " استفاده می گردد. تقویت کننده نوری از فیبرهای نوری متعدد بهمراه یک روکش خاص (doping) تشکیل می گردند. بخش دوپینگ با استفاده از یک لیزر پمپ می گردد . زمانیکه سیگنال تضعیف شده به روکش دوپینگی می رسد ، انرژی ماحصل از لیزر باعث می گردد که مولکول های دوپینگ شده، به لیزر تبدیل می گردند. مولکول های دوپینگ شده در ادامه باعث انعکاس یک سیگنال نوری جدید و قویتر با همان خصایص سیگنال ورودی تضعیف شده ، خواهند بود.(تقویت کننده لیزری)

دریافت کننده نوری

وظیفه دریافت کننده ، مشابه نقش ملوان بر روی عرشه کشتی ناو دریافت کننده پیام است. دستگاه فوق سیگنال های دیجیتالی نوری را اخذ و پس از رمزگشائی ، سیگنا ل های الکتریکی را برای سایر استفاده کنندگان (کامپیوتر ، تلفن و ...) ارسال می نماید. دریافت کننده بمنظور تشخیص نور از یک "فتوسل" و یا "فتودیود" استفاده می کند.

مزایای فیبر نوری

فیبر نوری در مقایسه با سیم های های مسی دارای مزایای زیر است :

- **ارزانتر**. هزینه چندین کیلومتر کابل نوری نسبت به سیم های مسی کمتر است .

- **نازک تر**. قطر فیبرهای نوری بمراتب کمتر از سیم های مسی است .
- **ظرفیت بال**ا. 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.

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)، (**OC3** Optical Carrier-3) (با سرعت ۱۵۵ مگابیت در ثانیه) دامنه وسیع خطوط اختصاصی را نشان می دهد. یک شبکه WAN دارای مزایای عمده ای نسبت به یک شبکه عمومی نظیر اینترنت از بعد امنیت وکارآئی است . پشتیانی و نگهداری یک شبکه WAN در عمل و زمانیکه 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 **VPN**) Virtual Network Private) 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 **VPDN**(Virtual private 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 **ESP**(service provider Enterprise) استفاده نمایند. سرویس دهنده ESP ، بمنظور نصب و پیکربندی VPN ، یک **NAS**(Network access server) 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 مهمترین 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 اختصای یک سازمان و اینترنت ایجاد می نماید. با استفاده از فایروال می توان عملیات متفاوتی را در جهت اعمال سیاست های امنیتی یک سازمان انجام داد. ایجاد محدودیت در تعداد پورت ها فعال ، ایجاد محدودیت در رابطه به پروتکل های خاص ، ایجاد محدودیت در نوع بسته های اطلاعاتی و ... نمونه هائی از عملیاتی است که می توان با استفاده از یک فایروال انجام داد.

● **رمزنگاری** . فرآیندی است که با استفاده از آن کامپیوتر مبداء اطلاعاتی رمزشده را برای کامپیوتر دیگر ارسال می نماید. سایر کامپیوترها ی مجاز قادر به رمزگشائی اطلاعات ارسالی خواهند بود. بدین ترتیب پس از ارسال اطلاعات توسط فرستنده ، دریافت کنندگان، قبل از استفاده از اطلاعات می بایست اقدام به رمزگشائی اطلاعات ارسال شده نمایند. سیستم های رمزنگاری در کامپیوتر به دو گروه عمده تقسیم می گردد :

- رمزنگاری کلید متقارن
- 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 Pretty Good Privacy(PGP) است . با استفاده از روش فوق می توان اقدام به رمزنگاری اطلاعات دلخواه خود نمود.

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

- روتر به روتر
- فایروال به روتر
- کامپیوتر به روتر
- کامپیوتر به سرویس دهنده

● **سرویس دهنده AAA** . سرویس دهندگان(**AAA** : Authentication Authorization,Accounting,) 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,L2F,PPTP,L2TP,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 یایت و دستیابی از راه دور) است . اینترفیش های Tunnel می بایست دارای امکانات حمایتی از IPSec باشند.

در شبکه های VPN از نوع " دستیابی از راه دور " ، Tunneling با استفاده از PPP انجام می گیرد. PPP 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:

- **F۲L**(Layer 2 Forwarding) . 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 .

PPTP(Tunneling Protocol Point-to-Point) . پروتکل فوق توسط کنسرسیومی متشکل از شرکت های متفاوت ایجاد شده است . این پروتکل امکان رمزنگاری ٤٠ بیتی و ١٢٨ بیتی را دارا بوده و از مدل های تعیین

اعتبار کاربر که توسط PPP حمایت شده اند ، استفاده می نماید.

L2TP - (Protocol Layer 2 Tunneling) . پروتکل فوق با همکاری چندین شرکت ایجاد شده است .پروتکل فوق از ویژگی های PPTP و L2F استفاده کرده است . پروتکل L2TP بصورت کامل IPSec را حمایت می کند. از پروتکل فوق بمنظور ایجاد تونل بین موارد زیر استفاده می گردد :

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

عملکرد Tunneling مشابه حمل یک کامپیوتر توسط یک کامیون است . فروشنده ، پس از بسته بندی کامپیوتر (پروتکل مسافر) درون یک جعبه (پروتکل کپسوله سازی) آن را توسط یک کامیون (پروتکل حمل کننده) از انبار خود (اینترفیس ورودی تونل) برای متقاضی ارسال می دارد. کامیون (پروتکل حمل کننده) از طریق بزرگراه (اینترنت) مسیر خود را طی ، تا به منزل شما (اینترفیش خروجی تونل) برسد. شما در منزل جعبه (پروتکل کپسول سازی) را باز و کامپیوتر (پروتکل مسافر) را از آن خارج می نمائید.