به نام خدا

جزوه آزمایشگاه شبکه

استاد: جناب آقای علی سلیمانی

تهیه کننده: هما اختیاری

دانشکده تهران غرب – مهندسی کامپیوتر تهران غرب

خرداد ۱۳۹۵

فهرست

عنوان صفحه

توپولوژی شبکه

تعریف توپولوژی

نحوه چینش و اتصال رایانه ها و اجزاء شبکه به یکدیگر و به عبارت دیگر طرح ساختار فیزیکی شبکه را توپولوژی شبکه می گویند.

انواع توپولوژی شبکه:

توپولوژی گذرگاه (BUS)
توپولوژی حلقوی (RING)
توپولوژی ستاره ای (STAR)
توپولوژی گراف (MESH)
توپولوژی درختی (TREE)
توپولوژی ترکیبی (Hybrid)

توپولوژی گذرگاه(BUS):

در حالت کلی از یک کابل به عنوان ستون فقرات اصلی در شبکه استفاده می‌شود و تمام کامپیوترهای موجود در شبکه سرویس دهنده (Server)، سرویس گیرنده (Client) به آن متصل می‌گردند. و سیگنال های اطاعات در طول مسیر کابل ارسال می گردد و تمام کامپیوتر هایی که به آن متصل هستند سیگنال ها را دریافت می نمایند.در این توپولوژی رسانه انتقال بین کلیه کامپیوتر ها مشترک است. توپولوژی BUS از متداولترین توپولوژی هاست که در شبکه های محلی مورد استفاده قرار می گیرد. در این روش کلیهٔ کامپیوترهای متصل به خط، اطلاعات ارسال شده را دریافت می‌کنند ولی فقط کامپیوتری که آدرس بسته اطلاعاتی ارسال شده، متعلق به او است این اطلاعات را ذخیره می‌نماید و بقیهٔ کامپیوترها از بسته صرف‌نظر می‌کنند.برای راه اندازی این آرایش خطی نیاز به کابل کواکسیال داریم و هر سیستم به کمک یک کانکتور به شبکه متصل می شود . ابتدا و انتهای شبکه با ترمیناتور بسته می شود.

مزایای توپولوژی BUS :

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

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

۳- توسعه آسان . یک کامپیوتر جدید را می‌توان به‌راحتی در نقطه ای ازشبکه اضافه کرد. در صورت اضافه شدن ایستگاههای بیشتر در یک سگمنت ، می‌توان از تقویت کننده هائی به نام Repeater استفاده کرد.

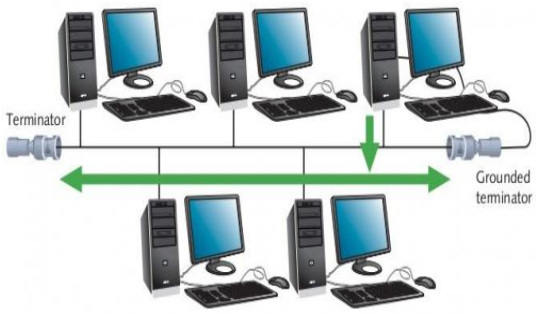
معایب توپولوژیBUS

۱- مشکل بودن عیب یابی . با اینکه سادگی موجود در تویولوژی BUS امکان بروز اشتباه را کاهش می‌دهند، ولی در صورت بروز خطا کشف آن ساده نخواهد بود. در شبکه‌هائی که از توپولوژی فوق استفاده می‌نمایند ، کنترل شبکه در هر گره دارای مرکزیت نبوده و در صورت بروز خطاء می‌بایست نقاط زیادی به منظور تشخیص خطا بازدید و بررسی گردند.

۲- ایزوله کردن خطاء مشکل است . در صورتی که یک کامپیوتر در توپولوژی فوق دچار مشکل گردد ، می‌بایست کامپیوتر را در محلی که به شبکه متصل است رفع عیب نمود. در موارد خاص می‌توان یک گره را از شبکه جدا کرد. در حالتی که اشکال در محیط انتقال باشد ، تمام یک سگمنت می‌بایست از شبکه خارج گردد. ضعف عمده این شبکه این است که اگر کابل اصلی که پل ارتباطی بین کامپیوتر های شبکه است ، قطع شود ، کل شبکه از کار خواهد افتاد.در این توپولوژی از کابل کواکسیال استفاده می شود.

۳- ماهیت تکرارکننده ها . در مواردی که برای توسعه شبکه از تکرارکننده‌ها استفاده می‌گردد، ممکن است در ساختار شبکه تغییراتی نیز داده شود. موضوع فوق مستلزم بکارگیری کابل بیشتر و اضافه نمودن اتصالات مخصوص شبکه است.

۴- اشکال دیگر این توپولوژی در آن است که هر یک از کامپیوتر ها باید برای ارسال پیام منتظر فرصت باشد. به عبارت دیگر در این توپولوژی در هر لحظه فقط یک کامپیوتر می تواند پیام ارسال کند.یکی دیگر از اشکالهای این توپولوژی است که تعداد کامپیوتر های واقع در شبکه تاثیر معکوس و شدیدی بر کارایی شبکه می گذارد. در صورتی که تعداد کاربران زیاد باشد، سرعت شبکه به مقدار قابل توجهی کند می شود. علت این امر آن است که در هر لحظه یک کامپیوتر باید برای ارسال پیام مدت زمان زیادی به انتظار بنشیند. عامل مهم دیگری که باید در نظر گرفته شود آن است که در صورت آسیب دیدگی کابل شبکه، ارتباط در کل شبکه قطع شود.



توپولوژی حلقوی (RING):

این نوع شبکه ها به صورت دایره ای شکل توسط یک مدیا به هم متصل شده اند.

Ring به معنای حلقه است و مانند این است که ابتدا و انتهای bus را به هم متصل کنیم.در این نوع توپولوژی هر کامپیوتر بصورت مستقیم به کامپیوتر بعدی در یک شبکه متصل میشود و بسته ی دیتا از کامپیوتری به کامپیوتر دیگر عبور می کند تا به مقصد برسد. وقتی کامپیوتری پیام را در یافت می کند ابتدا نشانی مقصد آن را بررسی میکند اگر نشانی پیام با نشانی کامپیوتریکسان باشد کامپیوتر پیام را می پذیرد در غیر اینصورت سیگنال را از نو تولید و پیام را برای کامپیوتر بعدی ارسال می کند. این تولید مجدد سیگنال به شبکه های Ring امکان می دهد که فواصل بزرگتری را نسبت به شبکه های خطی یا bus پوشش دهند.

برای ring یک سوئیچ مخصوص به نام mau ساختند دقیقا از لحاظ ساختاری شبیه سوئیچ بود اما از لحاظ ساختار درونی Ring می باشد. در این نوع شبکه ها وظیفه انتقال اطلاعات را بسته ای بنام token بر عهده دارد به همین دلیل به این شبکه token ring نیز گفته می شود.

Token به عنوان یک بسته خالی توسط یکی از کامپیوترهای شبکه به صورت اتوماتیک تولید می شود که این کامپیوترها را پروتکل tokenring بر اساس مشخصه هایی مثل شماره سریال یا آدرس کارت شبکه انتخاب می شود سپس token درون شبکه بصورت حلقوی شروع به حرکت می کند تا جایی که کامپیوتر درخواست ارسال اطلاعات را داشته باشد سپس اطلاعات به همراه آدرس فرستنده و گیرنده درون token قرار داده شده و دوباره token به حرکت خود ادامه میدهد تا به مقصد برسد در مقصد اطلاعات برداشته شده و بسته ای دیگر به token اضافه میشود تا صحت درستی دریافت اطلاعات را برای کامپیوتر فرستنده تایید کند . بسته دوباره در شبکه حرکت کرده تا به مبدا قبلی خود برسد در مبدا بسته بررسی شده و به همراه token حذف می شود . سپس کامپیوتر master دوباره token را تولید کرده و حرکت آن را در شبکه کنترل می کند . فرض کنید که در این ring توپی جا به جا می شود و هر کسی که تصمیم به ارسال اطلاعات دارد این توپ را در اختیار خود می گیرد و شروع به صحبت کردن می کند زمانی که بقیه می خواهند صحبت کنند دنبال توپ می گردند و وقتی که می بینند توپ نیست می فهمند که در اختیار کسی است.حال این توپ همان ولتاژ درون شبکه های bus را برای ما تداعی می کند. و همان ولتاژ ۳/۰ ولتی است که روی ring وجود دارد.

هر کسی که بخواهد صحبت کند دنبال ولتاژ ۰/۳ می گردد اگر که ولتاژ ۰/۳ بود یعنی کسی اطلاعاتی را ارسال نمی کند بنا براین token را در اختیار می گیرد. با در اختیار گرفتن token در اصل backbone را در اختیار خود گرفته است و ولتاژ را می تواند ۵ اهم برساند و زمانی که ارسال اطلاعات pc مربوط به تمام رسید ولتاژ به حالت اولیه ی خود باز می گردد و مابقی نیز می توانند اطلاعات را ارسال کنند.

حداکثر سرعت در توپولوژی ring چند است؟

حد اکثر سرعت ۱۶mb/s می باشد. در شبکه های ring جهت اتصال دو mau به یکدیگر باید port ring out یک mau را به port ring in – mau دیگر متصل کنیم

در شبکه ی ring نحوه ی ارسال اطلاعات به صورت half duplex می باشد.و دقیقا کامپیوتر ها به یک backbone متصل هستند و زمانی که یک کامپیوتر در حال ارسال اطلاعات است بقیه ی کامپیوتر ها کاری را انجام نمی دهند.

arbitration در توپولوژی ring چیست؟

نوع arbitration که در این نوع شبکه استفاده می شود token ring می باشد.

در این نوع توپولوژی ترتیب اتصال به mau بسیار حائز اهمیت است و pc ها باید به ترتیب mau متصل شوند.

مشکلاتی که در این توپولوژی هستند :

همه ی آنها halfduplex هستند و همه ی آنها داخل یک collision domain قرار می گیرند.

اگر در ring اتصالی به وجود آید کل شبکه قطع می شود.

و پایین بودن سرعت انتقال اطلاعات۱۶bps

توپولوژی ستاره ای(STAR):

در این توپولوژی همانگونه که از نام آن مشخص است ، از مدلی شبیه "ستاره" استفاده می گردد. وکلیه کامپیوتر ها به یک کنترل کننده مرکزی با هاب متصل هستند. هرگاه کامپیوتری بخواهد با کامپیوتر ی دیگری تبادل اطلاعات نماید، کامپیوتر منبع ابتدا باید اطلاعات را به هاب ارسال نماید. سپس از طریق هاب آن اطلاعات به کامپیوتر مقصد منتقل شود. اگر کامپیوتر شماره یک بخواهد اطلاعاتی را به کامپیوتر شماره ۳ بفرستد ، باید اطلاعات را ابتدا به هاب ارسال کند، آنگاه هاب آن اطلاعات را به کامپیوتر شماره سه خواهد فرستاد.

مزایای توپولوژی STAR :

۱- 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.

۲- در هر اتصال یک دستگاه :

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

۳- 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.

۴- 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:

۱- زیاد بودن طول کابل :

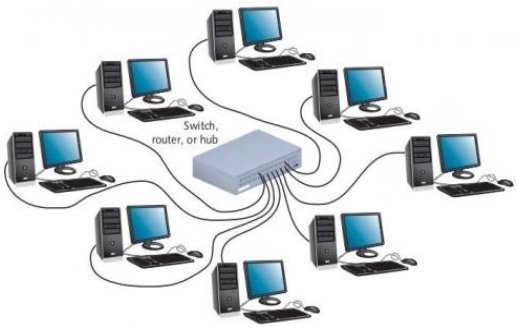
بدلیل اتصال مستقیم هر گره به نقطه مرکزی ، مقدار زیادی کابل مصرف می شود. با توجه به اینکه هزینه کابل نسبت به تمام شبکه ، کم است ، تراکم در کانال کشی جهت کابل ها و مسائل مربوط به نصب و پشتیبنی آنها بطور قابل توجهی هزینه ها را افزایش خواهد داد.

۲- 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.

۳- وابستگی به نقطه مرکزی . :

در صورتی که نقطه مرکزی (هاب) در شبکه با مشکل مواجه شود ، تمام شبکه غیرقابل استفاده خواهد بود.



توپولوژی گراف (MESH):

شبکه هایی که از توپولوژی مش استفاده می کنند، هر دستگاه را به کل دستگاه های شبکه متصل می نمایند.این شبکه ها سرعت بالایی دارند، چون هر گره مستقیما به تمام گره های دیگر شبکه متصل شده است و هیچ هابی به عنوان گلوگاه وجود ندارد. کابل کشی اضافی در این

شبکه ها، آن ها را گران کرده است و گره های جدید نمی توانند به سادگی اضافه شوند، زیرا باید به تمام گره ها وصل گردند.

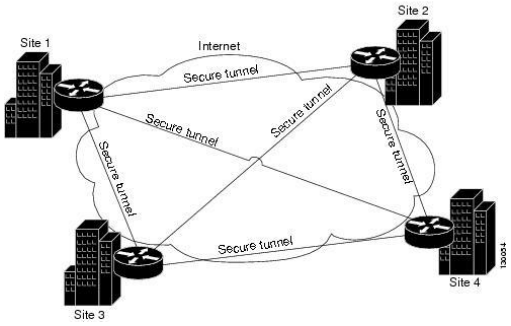
مزایای توپولوژی Mesh:

۱- این توپولوژی می توان به سرعت بالای انتقال اطلاعات نام برد چون سیستم ها در این توپولوژی به صورت مستقیم به هم متصل هستند .

معایب توپولوژی Mesh:

۱- از معایب این توپولوژی به حجم بالای کابل کشی می توان نام برد.

۲- از معایب دیگر این توپولوژی هزینه بالای پیاده سازی این شبکه نام برد.



توپولوژی درختی (TREE):

در آرایش درختی یک گره مرکزی (بالاترین سطح در سلسله مراتب) به دو یا چند گره در سطحی پایین تر با استفاده از یک پیوند نقطه به نقطه متصل است (به عنوان مثال در سطح دو) و گره‌های سطح دو نیز به چندین گره در سطحی پایینتر متصل هستند (برای مثال در سطح سوم). گره مرکزی تنها گرهی است که هیچ گرهی در سطحی بالاتر از خود ندارد. سلسله مراتب درخت متقارن است یعنی تعداد گره‌های متصل به هر گره در سطح پایین تر عدد ثابت f است. عدد f به عنوان عامل شاخه بندی در درخت سلسله مراتب شناخته می‌شود.

نکته ها:

۱- یک شبکه مبنی بر آرایش درختی فیزیکی حتماً باید حداقل سه سطح داشته باشد در غیر این صورت اگر دو سطح داشته باشد نشان دهنده آرایش ستاره است.

۲- اگر یک آرایش درختی عامل شاخه بندی برابر با یک داشته باشد این آرایش نشان دهنده آرایش خطی است.

۳- عامل شاخه بندی مستقل از تعداد کل گره هاست اگر یک گره نیاز به درگاه‌هایی برای اتصال به گره‌های دیگر داشته باشد می‌توان تعداد درگاه‌ها را بدون توجه به تعداد کل گره‌ها کاهش داد. در نتیجه تعداد درگاه‌های مورد نیاز وابسته به عامل شاخه بندی است و در نتیجه می‌توان تعداد درگاه‌ها را بدون توجه به تعداد کل گره‌ها کاهش داد.۴-

۴- تعداد کل پیوندهای نقطه به نقطه در شبکه بر اساس آرایش درختی یکی کمتر از تعداد گره‌های شبکه می‌باشد

۵- اگر نیاز به پردازش اطلاعات توسط گره‌ها در یک آرایش درختی فیزیکی باشد گره‌های سطح بالاتر باید پردازش بیشتری نسبت به گره‌های سطح پایین تر انجام دهند.

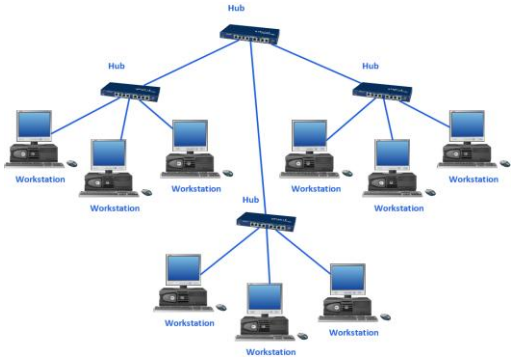
مزایای توپولوژی درختی :

۱- هزینه کمتر نسبت به mesh

۲- دارای کنترلهای مدیریتی بر زیر درختها-امکان ایجاد مسیرهای اضافی بین زیر درختهایی که کارایی بیشتری را برای آنها نیاز داریم.

معایب توپولوژی درختی :

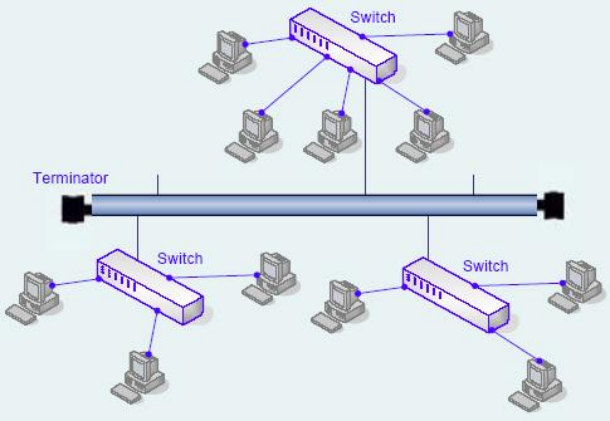
۱- قطع ارتباط قسمتی از شبکه در صورت قطعی خط مرتبط کننده آن زیر درخت با ریشه شبکه



توپولوژی ترکیبی (Hybrid):

از ترکیب توپولوژی های ستاره ای، حلقه ای و خطی، یک توپولوژی ترکیبی (Hybrid) به دست می آید. از توپولوژی هیبرید در شبکه های بزرگ استفاده می شود. خود توپولوژی هیبرید دارای دو نوع است. نوع اول توپولوژی خطی - ستاره ای نام دارد. همانطور که از نام آن بر می آید، در این آرایش چندین شبکه ستاره ای به صورت خطی به هم ارتباط داده می شوند. در این وضعیت اختلال در کارکرد یک کامپیوتر، تاثیر در بقیه شبکه ایجاد نمی کند. ضمن آنکه در صورت از کار افتادن هاب فقط بخشی از شبکه از کار خواهد افتاد. در صورت آسیب دیدگی کابل اتصال دهنده هاب ها، فقط ارتباط کامپیوتر هایی که در گروه های متفاوت هستند قطع خواهد شد و ارتباط داخلی شبکه پایدار می ماند. نوع

دوم نیز توپولوژی ستاره ای - حلقه ای نام دارد. در این توپولوژی هاب های چند شبکه از نوع حلقه ای در یک الگوی ستاره ای به یک هاب مرکزی متصل می شوند.



انواع کابل شبکه

۱. کابل های هم محور یاCoaxial
۲. کابل های زوجی یا هشت سیمی
۳. فیبر نوری

کابلهای کواکسیال

این کابلها همان کابل آنتن تلویزیون خانگی هستند و در شبکه باس استفاده می شوند. کابلهای کواکسیال که در شبکه باس بکار میرود به دو نوع کلی Thin و Thick تقسیم می‌شود که نوع دوم دیگر استفاده نمی شود.برای اتصال این کابل به کارت شبکه از کانکتور های BNC و T connector استفاده میشود.

کابل زوجی یا هشت سیمی

این کابل ها مرسوم ترین کابل در ایجاد شبکه های کامپیوتری مانند اترنت هستند. این نوع کابل در هفت دسته بندی یا categoryکه به اختصار cat نیز گفته می شود وجود دارند. کابل های زوجی ممکن است بدون محافظ باشند و به آنها UTP گویند. کابلهای دارای شیلد یا STP نیز در مکانهائی مانند اسانسور یا کنار کابل های فشارقوی برق که نویز وجود دارد استفاده می شود.

کانکتور استاندارد برای کابل های UTP ، از نوع RJ-45 می باشد. این کانکتور شباهت زیادی به کانکتورهای تلفن (RJ-11) دارد. واژه RJ نیز مخفف Registered Jack است.

کانکتور استاندارد برای کابل های کواکسیال، از نوع BNC یا Bayone Neill Concelman می باشد.

کابل هایUTP: Unshielded Twisted Pair

کابل UTP یکی از متداولترین کابل های استفاده شده در شبکه های مخابراتی و کامپیوتری است . از کابل های فوق ، علاوه بر شبکه های کامپیوتری در سیستم های تلفن نیز استفاده می گردد .(CAT1) شش نوع کابل UTP متفاوت وجود داشته که می توان با توجه به نوع شبکه و اهداف مورد نظر از آنان استفاده نمود .

کابلCAT5 ، متداولترین نوع کابل UTP محسوب می گردد.
با توجه به مشخصه های کابل های UTP ، امکان استفاده ، نصب و توسعه سریع و آسان آنان ، فراهم می آورد . جدول زیر انواع کابل های UTP را نشان می دهد:

گروه	سرعت انتقال اطلاعات	موارد استفاده
CAT1	حداکثر تا یک مگابیت در ثانیه	سیستم های قدیمی تلفن ، ISDN و مودم
CAT2	حداکثر تا چهار مگابیت در ثانیه	شبکه های Token Ring
CAT3	حداکثر تا ده مگابیت در ثانیه	شبکه های Token ring و BASE-T۱۰
CAT4	حداکثر تا شانزده مگابیت در ثانیه	شبکه های Token Ring
CAT5	حداکثر تا یکصد مگابیت در ثانیه	اترنت (ده مگابیت در ثانیه) ، اترنت سریع (یکصد مگابیت در ثانیه) و شبکه های Token Ring (شانزده مگابیت در ثانیه)
CAT5e	حداکثر تا یکهزار مگابیت در ثانیه	شبکه های Gigabit Ethernet
CAT6	حداکثر تا یکهزار مگابیت در ثانیه	شبکه های Gigabit Ethernet

توضیحات :

- تقسیم بندی هر یک از گروه های فوق بر اساس نوع کابل مسی و Jack انجام شده است ..
- از کابل های گروه CAT2, CAT3, CAT4, CAT5 و CAT6 در شبکه ها استفاده می گردد .کابل های فوق ، قادر به حمایت از ترافیک تلفن و شبکه های کامپیوتری می باشند .
- برای شبکه هائی با سرعت بالا (یکصد مگا بیت در ثانیه) از کابل های CAT5 و برای سرعت ده مگابیت در ثانیه از کابل های CAT3 استفاده می گردد.
- حداکثر مسافت در کابل های CAT3 ، یکصد متر است .
- حداکثر مسافت در کابل های CAT4 ، دویست متر است .
- کابل CAT6 با هدف استفاده در شبکه های اترنت گیگابیت طراحی شده است . در این رابطه استانداردهائی نیز وجود دارد که امکان انتقال اطلاعات گیگابیت بر روی کابل های CAT5 را فراهم می نماید(CAT5e) .کابل های CAT6 مشابه کابل های CAT5 بوده ولی بین ۴ زوج کابل آنان از یک جداکننده فیزیکی به منظور کاهش پارازیت های الکترومغناطیسی استفاده شده و سرعتی بالغ بر یکهزار مگابیت در ثانیه را ارائه می نمایند.

کابل های کراس CAT5 UTP که از آنان با نام X-over نیز نام برده می شود ، یکی از متداولترین کابل های استفاده شده پس از کابل های Straight می باشند . با استفاده از کابل های فوق ، می توان دو کامپیوتر را بدون نیاز به یک هاب و یا سوئیچ به یکدیگر متصل نمود. با توجه به این که هاب عملیات X-over را به صورت داخلی انجام می دهد ، در زمانی که یک کامپیوتر را به یک هاب متصل می نمائیم ، صرفا" به یک کابل Straight نیاز می باشد . در صورتی که قصد اتصال دو کامپیوتر به یکدیگر را بدون استفاده از یک هاب داشته باشیم ، می بایست عملیات X-over را به صورت دستی انجام داد و کابل مختص آن را ایجاد نمود.

کابل CAT5 X-over

به منظور ایجاد کابل های کراس CAT5 صرفا" از یک روش استفاده می گردد. همانگونه که قبلا" اشاره گردید ، یک کابل X-over پین TX یک سمت را به پین RX سمت دیگر متصل می نماید(و برعکس) . شکل زیر شماره پین های یک کابل CAT5معمولی X-over را نشان می دهد.

شماره پین های یک کابلCAT5 X-over

همانگونه که در شکل فوق مشاهده می گردد در کابل های X-over صرفا" از پین های شماره یک ، دو ، سه و شش استفاده می گردد . پین های یک و دو بمنزله یک زوج بوده و پین های سه و شش زوج دیگر را تشکیل می دهند . از پین های چهار ، پنج ، هفت و هشت استفاده نمی گردد . (صرفا" از چهار پین برای ایجاد یک کابل X-over ، استفاده می گردد) .

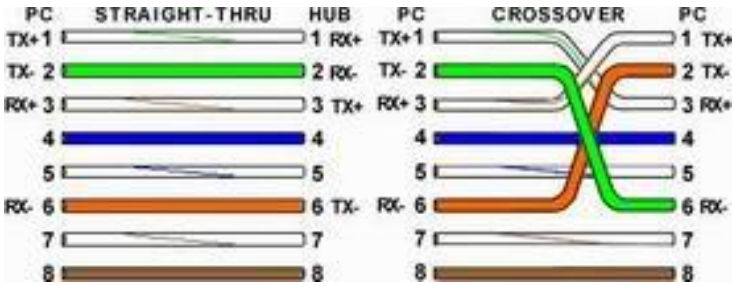
موارد استفاده از کابل های X-over

از کابل های X-over صرفا" به منظور اتصال دو کامپیوتر استفاده نمی شود و می توان از آنان در دستگاه های متفاوتی نظیر سوئیچ و یا هاب نیز استفاده نمود . در صورتی که قصد داشته باشیم دو هاب را به یکدیگر متصل نمائیم ، معمولا" از پورت uplinkاستفاده می گردد. پورت فوق ، بخش های tx و rx را کراس نمی نماید. شکل زیر نحوه اتصال دو هاب به یکدیگر با استفاده از یک کابل Straight و از طریق پورت Uplink را نشان می دهد

اتصال دو هاب با استفاده از پورت Uplink و یک کابلStraight

با توجه به وجود پورت uplink ، نیازی به استفاده از یک کابل x-over نخواهد بود . در صورتی که امکان استفاده از پورت uplinkوجود نداشته باشد و بخواهیم دو هاب را با استفاده از پورت های معمولی به یکدیگر متصل نمائیم ، می توان از یک کابل X-over استفاده نمود . شکل زیر نحوه اتصال دو هاب به یکدیگر با استفاده از یک کابل X-over را و بدون استفاده از پورت Uplink نشان می دهد:

شکل زیر تفاوت موجود بین شماره پین های یک کابل Straight و X-over را نشان می دهد:



کابل کشی شبکه : ایجاد کابل Straight

کابل کشی شبکه یکی از مراحل مهم در زمان پیاده سازی یک شبکه کامپیوتری است که می بایست با دقت،ظرافت خاص و پایبندی به اصول کابل کشی ساختیافته ، انجام شود. برای ایجاد کابل های UTP از تجهیزات زیر استفاده می گردد:

مدل های متفاوت کابل کشی کابل های UTP

به منظور کابل کشی کابل های UTP از دو استاندارد متفاوت T-568A و T-568B استفاده می گردد . نحوه عملکرد دو مدل فوق یکسان بوده و تنها تفاوت موجود به رنگ زوج هائی است که به یکدیگر متصل می شوند.در کابل های UTP از کانکتورهای استاندارد و چهار زوج سیم بهم تابیده استفاده می گردد :

- زوج اول : آبی و سفید/ آبی
- زوج دوم : نارنجی و سفید /نارنجی
- زوج سوم : سبز و سفید/ سبز
- زوج چهارم : قهوه ای و سفید / قهوه ای

در شبکه های ۱۰/۱۰۰ Mbit از زوج های دو و سه استفاده شده و زوج های یک و چهار رزو شده می باشند . در شبکه های گیگااترنت از تمامی چهار زوج استفاده می گردد. کابل های CAT5 متداولترین نوع کابل UTP بوده که دارای انعطاف مناسب بوده و نصب آنان بسادگی انجام می شود.

ایجاد یک کابل UTP به منظور اتصال کامپیوتر به هاب (معروف به کابل های Straight)

اترنت عموما" با استفاده از هشت کابل هادی به همراه هشت پین ماژولار plugs/jacks ، داده را حمل می کند . کانکتور استاندارد، RJ-45 نامیده شده و مشابه کانکتور استاندارد RJ-11 است که در تلفن استفاده می گردد. یک رشته کابل CAT5 شامل چهار زوج سیم بهم تابیده است که هر زوج دارای دو رشته سیم با رنگهائی خاص است . (یک رشته رنگی و یک رشته سفید با نواری به رنگ رشته زوج مربوط) . به منظور تسهیل در امر نگهداری ، می بایست به اندازه ضروری سیم های بهم تابیده را از حالت پیچش خارج نمود (مثلا" حدود یک سانتیمتر) . زوج های در نظر گرفته شده برای اترنت ده و یکصد مگابیت به رنگ نارنجی و سبز می باشند . از دو زوج دیگر (رنگ قهوه ای و آبی) می توان به منظور یک خط اترنت دوم و یا اتصالات تلفن استفاده نمود .

به منظور کابل کشی کابل های UTP از دو استاندارد متفاوت با نام T-568B (یا EIA) و T-568A (یا T &AT، 258A) ، استفاده می گردد . تنها تفاوت موجود بین آنان ترتیب اتصالات است .

فیبر نوری

فیبر نوری یا تار نوری به انگلیسی (Optical Fiber) رشته باریک و بلندی از یک مادّه شفاف مثل شیشه یا پلاستیک است که می‌تواند نوری را که از یک سرش به آن وارد شده، از سر دیگر خارج کند. فیبر نوری داری پهنای باند بسیار بالاتر از کابل‌های معمولی می‌باشد، با فیبر نوری می‌توان داده‌های تصویر، صوت و داده‌های دیگر را به راحتی با پهنای باند بالا تا ۱۰ گیگابیت بر ثانیه و بالاتر انتقال دادمروزه مخابرات فیبر نوری، به دلیل پهنای باند وسیعتر در مقایسه با کابلهای مسی، و تاخیر کمتر در مقایسه با مخابرات ماهواره ای از مهمترین ابزار انتقال اطلاعات محسوب می‌شود.

۱. کاربرد در مخابرات: یکی از مرسوم ترین کاربردهای فیبر نوری انتقال اطلاعات توسط نور لیزر است.

۲. کاربرد در حسگرها: استفاده از حسگرهای فیبر نوری برای اندازه‌گیری کمیت‌های فیزیکی مانند جریان الکتریکی، میدان مغناطیسی، فشار، حرارت، جابجایی، آلودگی آب‌های دریا، سطح مایعات، تشعشعات پرتوهای گاما و ایکس در سال‌های اخیر شروع شده‌است. در این نوع حسگرها، از فیبر نوری به عنوان عنصر اصلی حسگر بهره‌گیری می‌شود بدین ترتیب که ویژگی‌های فیبر تحت میدان کمیت مورد اندازه‌گیری تغییر یافته و با اندازه شدت کمیت تأثیرپذیر می‌شود.

۳. کاربردهای نظامی: فیبر نوری کاربردهای بی‌شماری در صنایع دفاع دارد که از آن جمله می‌توان برقراری ارتباط و کنترل با آنتن رادار، کنترل و هدایت موشک‌ها، ارتباط زیردریاییها (هیدروفون) را نام برد.

۴. کاربردهای پزشکی: فیبرنوری در تشخیص بیماری‌ها و آزمایشهای گوناگون در پزشکی کاربرد فراوان دارد که از آن جمله می‌توان دُزیمتری غدد سرطانی، شناسایی نارسایی‌های داخلی بدن،جراحی لیزری، استفاده در دندانپزشکی و اندازه‌گیری مایعات و خون نام برد. همچنین تارهای نوری در دستگاه‌هایی به نام درون بین یا آندوسکوپ استفاده می‌شود تا به درون نای، مری، روده ومثانه فرستاده شود و درون بدن انسان به طور مستقیم قابل مشاهده باشد.

۵. کاربرد فیبرنوری در روشنایی: از جمله کاربردهای فیبر نوری که در اواخر قرن بیستم به عنوان یک فناوری روشنایی متداول شده و در چند سال قرن اخیر توسعه و رشد فراوانی پیدا کرده‌است کاربرد آن در سیستم‌های روشنایی است. در این فناوری نور از منبع نوری که می‌تواند نور مصنوعی (نورلامپهای الکتریکی) و یا نور طبیعی (نور خورشید) باشد وارد فیبر نوری شده و از این طریق به محل مصرف منتقل می‌شود. به این ترتیب نور به هر نقطه‌ای که در جهت تابش مستقیم آن نمی‌باشد منتقل می‌شود. امتیاز این نور که موجبات رشد سریع به کارگیری و توجه زیاد به این فناوری شده‌است این است که فاقد الکتریسیته گرما و تشعشعات خطرناک ماورای بنفش بوده (نور خالص و بی خطر) و دیگر اینکه بااین فناوری می‌شود نور روز (بدون گرما واشعه‌های ماورائ بنفش) را هم به داخل ساختمانها و نقاط غیر قابل دسترسی به نور خورشید منتقل کرد.

ابزارهای شبکه

ابزارهای زیادی را می توان به منظور عیب یابی و پیاده سازی شبکه بکارگرفت تستر کابل و ابزارهای TDR/OTDR از این جمله هستند.

تستر کابلCable Tester / Certifier

در اینجا تصویری از ابزار تستر کابل قرار دادیم ولی این را بدانید که هیچ تصویر مشخصی از این ابزار وجود ندارد و انواع مختلفی دارد و تمرکز شما بایستی بیشتر به عملکرد آنها باشد.

Cable Testerتستر کابل همانگونه که از نام آن پیداست برای تست عملکرد درست کابل استفاده می شود . در بسیاری از مواقع پس از اینکه دو طرف کابل را سوکت زنی کردید برای اینکه از کار خود مطمئن شوید می توانید از تستر کابل استفاده کنید Certifierابزاری است که برای تایید سطح توان عملیاتی کابل استفاده می شود . به عنوان مثال ممکن است شما شبکه ای با استاندارد Ethernet 100Mb را داشته باشید و بخواهید آن را به شبکه گیگابیت ارتقا دهید برای این ارتقا ابتدا نیاز است تا توان عملیاتی کابل شما تست و بررسی شود.

تشخیص پیوستگی کابل TDR / OTDR

TDRمخفف Time Domain Reflectometer و OTDR مخفف Optical Time Dmain Reflectometer می باشد . وظیفه اصلی این دو ابزار این است که تشخیص دهند که آیا کابل از پیوستگی برخوردار است یا خیر با این تفاوت که TDRاین کار را در کابل های مسی انجام می دهد و OTDR در کابل های فیبرنوری.

این دو ابزار گام را از این فراتر گذاشته و حتی محل قطع یا حتی خراشیدگی کابل را برای شما مشخص می کند . فرض کنید در ساختمان بزرگی کابل قطع شده و کابل از پشت دیوار و سقف عبور داده شده است . بدون این ابزار شما بایستی کل ساختمان را خراب کنید تا محل خرابی کابل را پیدا کنید , در حالی که با استفاده از این ابزار محل خرابی کابل تعیین می شود و فقط ناحیه مورد نظر پیاده سازی می گردد.

آچرشبکه:

وسیله ایست جهت پرس کردن سوکت شبکه به سیم شبکه ، اصولا دو قسمت برای پرس در آچار موجود است یکی برای RJ11 که ۶ پین و مورد استفاده در تلفن و مخابرات می‌باشد و یکی۸ پین جهت پرس RJ45 مورد استفاده در شبکه که علاوه بر فشردن پین‌های شبکه بر روی سیم‌های قرارداده شده قسمت تهدانی سوکت را هم به قلاف محافظ سیم شبکه پرس میکند تا از سوکت جدا نشود

.

آچار پانچ:

از این نوع آچار برای پانچ کردن سیم های شبکه و مخابراتی در داخل ترمینال ها ، کیستون ها و پچ پنل های غیر ماژولار استفاده می شود . همزمان با پرس سیم در محل خود ، اضافه سیم نیز توسط آچار قطع می شود. در دو نوع قیچی دار که عملیات چیدن اضافه سیم توسط تیغ آچار انجام می شود . برخی از انواع آن دارای پیچ تنظیم فشار هستند و برخی نیز دارای قلاب کمری می باشند

.

تست OTDR

تست OTDRیا بازتاب سنج نوری برای آزمایش سالم بودن کابل فیبر نوری به کار می رود که می تواند اتلاف اتصال را بررسی، طول را اندازه گیری و عیوب را پیدا کند OTDR .معمولا برای ایجاد یک تصویر از کابل فیبر نوری در مراحل نصب آن استفاده می شود. پس از آن در صورت وجود مشکلات، مقایسه ای بین طرح اصلی و طرح دوم صورت می گیرد.
تجزیه وتحلیل طرح OTDR به دلیل وجود مستندات طرح اصلی که در زمان نصب کابل ایجاد شده است آسان می باشد .
OTDRبرای تست کابل های طولانی (بیش از ۲۵۰ متر به صورت تقریبی یا ۸۰۰ فوت) یا کابل های فیوژن شده بسیار موثر می باشد.
داده ای که OTDR به وجود می آورد معمولا برای تولید یک عکس که trace نامیده می شود استفاده می شود که اطلاعات با ارزشی را در اختیار کاربر آموزش دیده قرار می دهد و می تواند این اطلاعات را برای ارجاع بعدی به طرح در صورت ایجاد مشکل در شبکه ذخیره کند.
تست OTDR نباید برای اندازه گیری اتلاف الحاقی در کابل فیبر نوری استفاده شود. این کار بهتر است توسط منبع آزمایش فیبر نوری و نیرو سنج انجام شود. دستگاه OTDR به سادگی به شما نشان می دهد که کابل ها کجا ترمینال شده اند و کیفیت فیبر

ها و اتصالات و جوش ها را تایید می کند. البته طرح های OTDR معمولا برای عیب یابی استفاده می شوند به دلیل اینکه آنها می توانند مکان شکستگی فیبر را در زمان مقایسه طرح ها با مستندات نصب، نشان دهند.

دستگاه OTDR دارای ۲ مدل رایج می باشد که در زیر به شرح آنها می پردازیم:

OTDR با تمام امکانات

دستگاه OTDR با تمام ویژگی ها یک دستگاه بازتاب سنج نوری قدیمی می باشد .که دارای تمام ویژگی ها بوده و نسبت به مدل های دیگر بزرگتر، سنگینتر و با امکان حمل دشوارتری می باشد. با وجود اینکه به بزرگی و سنگینی معروف می باشد اما ابعاد و وزن آن در مقایسه با نسل اولیه OTDR خیلی کمتر می باشد .اغلب این دستگاه ها یک قالب اصلی دارند که می توانند با واحد های پلاگین چند منظوره برای انجام بسیاری از اندازه گیری های فیبر تجهیز شوند. همچنین دارای صفحه نمایش رنگی بزرگ می باشند. این مدل اغلب دارای محدوده اندازه گیری بیشتری از سایر مدل ها می باشد و بیشتر در آزمایشگاه ها و اندازه گیری های دشوار فیبر استفاده می شوند. منبع تغذیه بیشتر این دستگاه ها جریان AC و یا باطری می باشد.

OTDR •دستی و جستجوگر شکستگی در فیبر

OTDRدستی (کوچک) و جستجوگر شکستگی در فیبر برای عیب یابی شبکه های فیبر در زمینه محیطی طراحی شده اند که اغلب از باطری استفاده می کنند. این نوع OTDRارزان قیمت و سبک وزن بوده و استفاده از آن آسان می باشد. این دستگاه تجزیه تحلیل داده های ابتدایی را انجام می دهد و ویژگی های کمتری از دستگاه های قبلی دارند. این دستگاه ها اغلب می توانند در ارتباط با نرم افزار های مبتنی بر pc برای انجام جمع اوری اطلاعات و تجزیه و تحلیل داده های پیچیده استفاده شوند.
OTDRهای دستی معمولا برای اندازه گیری لینک فیبر ها ، پیدا کردن شکستگی فیبر، نقاط با اتلاف بالا، اتلاف انتها به انتها و اتلاف بازگشت نور (ORL) استفاده می شوند.
دستگاه هایی که شکستگی فیبر را پیدا می کنند ابزار هایی کم هزینه می باشند که مخصوص پیدا کردن محل رویداد های مشکل ساز فیبر مانند شکستگی فیبر، نقطه انعکاس بالا یا اتلاف بالا طراحی شده اند.
این دستگاه نوار اندازه گیری الکترونیکی- نوری می باشد که فقط جهت اندازه گیری فاصله رویداد های مشکل ساز فیبر طراحی شده اند.
به طور کلی دستگاه های OTDR دستی و دستگاه جستجوگر شکستگی در فیبر سبکتر و کوچکتر ، دارای کاربرد آسانتر نسبت به دستگاه های کامل می باشند و اکثرا از باطری استفاده می کنند.
هدف این دو دستگاه این است که برای کارشناسان فنی ارزان و به عنوان ابزاری استاندارد باشد.

تستر کابل شبکه،همانگونه که از نام آن پیداست برای تست عملکرد درست کابل های شبکه استفاده می شود . در بسیاری از مواقع پس از اینکه دو طرف کابل را سوکت زنی کردید برای اینکه از کار خود مطمئن شوید می توانید از این دستگاه استفاده کنید .

برای نمونه فرض کنید در ساختمانی ۴ طبقه در هر طبقه ۲۴ گره یا Node شبکه وجود داشته باشد. کابل ها درون کانال های ویژه دیوارها کار گذاری شده اند و حدود ۲۵۰۰ متر کابل مصرف شده است. پس از اتصال رایانه ها به شبکه برخی از آنها به شبکه داخل Login نمی شوند. حتی تصور آن که باید چنین شبکه ای را (که تازه دارای مقیاسی خیلی بزرگی هم نمی باشد.) بدون تستر مورد بررسی قرار داد و پس از عیب یابی به رفع آن اقدام نمود سر را گیج می کند!! اینجاست که اهمیت فوق العاده دستگاه های عیب یاب و تستر شبکه ارزشمندی کار آنان نمایان می گردد.

تستر های شبکه در واقع دو دستگاه در یک دستگاه هستند که قالبا از هم جدا میشود و به شما این امکان را میدهند تا با قرار دادن دو سر کابل در دو سر دستگاه از درست بودن لینک و سالم متصل بودن سوکت ها به کابل اطمینان حاصل کنید.

به طور کلی سرعت و کیفیت جابجایی اطلاعات بر روی بستر شبکه را میتوان اندازه گیری نمود ، تستر کابل شبکه-تست فلوک- یکی از ابزارهای اندازه گیری و تست ارتباطات کابلی بر روی شبکه های کامپیوتری است.میزان اطلاعاتی که انواع مختلف این تسترها در اختیار کاربران آن قرار می دهد با توجه به نوع آن وسیله متغیر است ، از جمله اطلاعاتی که یک تستر خوب در اختیار کارشناسان کابل کشی قرار میدهد احتمال قطعی در طول مسیر و میزان متراژ می باشد.

تست فلوک نمونه ای از این نوع تست ها می باشد که با بهره گیری از محصولات شرکت FLUKE صورت می گیرد برتری این نوع تست نسبت به سایر نمونه های مشابه از آنجایی است که میزان خروجی اطلاعات از این دستگاه به مراتب بیشتر از سایر تستر ها میباشد . در این نوع تست علاوه بر امکان سنجی ای که روی کابل ها انجام می شود تجهیزات و اتصالات طول مسیر و استانداردهای لازم نیز مورد بررسی قرار می گیرد و در درون دستگاه ذخیره میگردد و در نهایت میتوان گزارشی کامل را در اختیار داشت.

مواردی که در ادامه لیست شده اند عمده ی اطلاعاتی است که این نوع تستر ها در اختیارتان می گذارند:

–تست دقیق و کامل لایه فیزیکی شبکه شامل کابل ، کیستون پریز ، پچ پنل ، پچ کابل
–تایید اصلی یا غیراصلی بودن تجهیزات پسیو شبکه (کابل ، کیستون ، پچ پنل ، پچ کابل)
–استخراج متراژ دقیق کابل کشی‌ها گزارش اشکالات اتصالات پچ‌پنل و کیستون
–گزارش قطع بودن یا ضعیف بودن نحوه اتصال رشته‌های کابل به کیستون
–گزارش وجود نویز ومحل دقیق آن در مسیر کابلکشی
–گزارش وجود کشش یا خمش بیش از حد و محل دقیق آن در مسیر کابلکشی
–گزارش میزان خلوص مس بکار رفته در کابل شبکه تست مقاومت و میزان رسانایی کابل
–اندازه گیری پارامترهای فیزیکی و مفهومی لینک از قبیل:

Propagation Delay
Length
Wire Map
Dc loop Resistance
Delay Skew
EXT
eturn Loss-RL
Insertion Loos
CR

در خصوص اهمیت دستگاه تستر فلوک و گزارش تستهای آماری این دستگاه میتوان به این نکته اشاره کرد که کلیه وزارتخانه ها و ادارات کل و سازمانها در برگزاری مناقصات اجرای شبکه های مسی ، فیبر نوری یکی از شرایط اولیه و ضروری شرکت در مناقصات را بهره مندی از ابزار نصب و تست و آنالیز مورد نیاز از جمله دستگاه تستر فلوک اعلام می نمایند.

کلاس های ip

طراحی یک مدل آدرس دهی IP منطبق بر طرح شبکه

آدرس IP ، یک شناسه عددی است که به هر ماشین موجود بر روی یک شبکه IP نسبت داده می شود . آدرس فوق ، مکان خاص یک دستگاه بر روی شبکه را مشخص می نماید . آدرس IP یک آدرس نرم افزاری است (نه یک آدرس سخت افزاری) . هر اینترفیس شبکه دارای یک آدرس سخت افزاری نیز می باشد که از آن به منظور یافتن هاست بر روی یک شبکه محلی استفاده می گردد . آدرس دهی مبتنی بر IP ، امکان مبادله اطلاعات بین هاست موجود در یک شبکه محلی با هاست موجود بر روی شبکه دیگر صرف نظر از نوع شبکه محلی را فراهم می نماید .

در زمان طراحی مدل آدرس دهی IP در یک شبکه ، می بایست به مواردی متعددی توجه شود چراکه با در نظر گرفتن برخی ملاحظات در زمان طراحی ، نگهداری شبکه در مدت زمان حیات آن راحت تر می گردد .

اصطلاحات IP

- بیت (bit) : یک بیت شامل یک رقم است . صفر و یا یک
- بایت (byte) : یک بایت بسته به این که از parity استفاده شده باشد از هفت و یا هشت بیت تشکیل می گردد . در ادامه همواره فرض ما بر این است که یک بایت از هشت بیت تشکیل شده است .
- اکتت (octet) : یک اکتت از هشت بیت تشکیل می گردد و صرفا" یک عدد هشت بیتی در مبنای دو را نشان می دهد . در ادامه به دفعات از واژه های بایت و اکتت به جای هم استفاده شده است .
- آدرس شبکه (Network address) : از آدرس شبکه به منظور روتینگ و ارسال بسته های اطلاعاتی به یک شبکه راه دور استفاده می شود . آدرس های ۰ . ۰ . ۰ . ۱۰ و ۰ . ۱۰ . ۱۶۸ . ۱۹۲ نمونه هائی در این زمینه می باشند .
- آدرس پخش (Broadcast address) : از آدرس های فوق ، برنامه ها و هاست ها جهت ارسال اطلاعات برای تمامی هاست های موجود در یک شبکه استفاده می نمایند .
  ۲۵۵ . ۲۵۵ . ۲۵۵ . ۲۵۵ تمامی شبکه ها و تمامی گره ها
  ۲۵۵ . ۲۵۵ . ۱۶ . ۱۷۲ تمام subnet و هاست ها بر روی شبکه ۰ . ۰ . ۱۶ . ۱۷۲
  ۲۵۵ . ۲۵۵ . ۲۵۵ . ۱۰ به تمامی subnet و هاست موجود بر روی شبکه ۰ . ۰ . ۰ . ۱۰
  نمونه هائی از آدرس های broadcast می باشند .

مدل آدرس دهی سلسله مراتبی IP

یک آدرس IP شامل ۳۲ بیت اطلاعات است . این بیت ها به چهار بخش تقسیم می گردند که به هر بخش بایت و یا اکتت گفته می شود . هر بایت و اکتت شامل هشت بیت می باشد . برای نمایش یک آدرس IP می توان از روش های متعددی استفاده نمود :

- دهدهی - جدا شده توسط نقطه (۵۶ . ۳۰ . ۱۶ . ۱۷۲)
- باینری یا مبنای دو (۰۰۱۱۱۰۰۰ . ۰۰۰۱۱۱۱۰ . ۰۰۰۱۰۰۰۰ . ۱۰۱۰۱۱۰۰)
- مبنای شانزده (AC.10.1E.38)

تمامی مثال های فوق یک آدرس IP مشابه را نمایش می دهند . در زمان بحث بر روی آدرس دهی IP از مبنای شانزده به میزانی که از "دهدهی - جدا شده توسط نقطه" و یا باینری استفاده می شود ، استفاده نمی گردد . در برخی برنامه ها ممکن است از یک

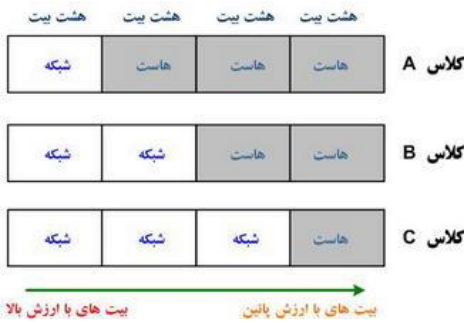
آدرس IP به صورت مبنای شانزده استفاده گردد . ریجستری ویندوز یک نمونه مناسب از برنامه هائی است که آدرس IP ماشین را به صورت مبنای شانزده ذخیره می نماید .
آدرس سی و دو بیتی IP ، یک آدرس ساختیافته و یا سلسله مراتبی است (در مقابل آدرس های غیرسلسله مراتبی و flat) . با این که می توان از هر نوع مدل آدرس دهی استفاده نمود ، ولی توصیه می گردد که از آدرس دهی سلسله مراتبی استفاده شود . ارائه تعداد بسیار زیادی آدرس ، مزیت عمده استفاده از یک مدل آدرس دهی سلسله مراتبی است . با توجه به این که آدرس IP سی و دو بیتی است و هر بیت می تواند مقدار صفر و یا یک را دارا باشد ، در مجموع دو به توان سی و دو آدرس را خواهیم داشت (۴ / ۳ میلیارد و یا ۴،۲۹۴،۹۶۷،۲۹۶) .
اشکال مدل آدرس دهی flat و علت عدم استفاده از آن برای آدرس دهی IP به روتینگ مربوط می گردد . در صورتی که هر آدرس منحصربفرد باشد ، تمامی روترهای موجود در اینترنت می بایست آدرس هر ماشین موجود در اینترنت را ذخیره نمایند . این موضوع روتینگ موثر را غیرممکن می سازد حتی اگر صرفا" بخشی از آدرس های موجود استفاده شده باشد .
برای حل این مشکل می توان از مدل آدرسی دهی سلسله مراتبی با دو و یا سه سطح استفاده نمود که در آن آدرس ها بر اساس شبکه ، هاست (دو سطح) و یا شبکه ، زیر شبکه و هاست (سه سطح) سازماندهی می شوند .
مدل آدرس دهی سلسله مراتبی (با دو و یا سه سطح) را می توان با یک شماره تلفن مقایسه نمود . در یک شماره تلفن ، بخش اول مربوط به کد شهر است . بخش دوم مربوط به یک ناحیه محلی در شهر مورد نظر است و بخش نهائی شماره مشترک است .
آدرس های IP از یک ساختار لایه ای مشابه استفاده می نمایند . در مقابل این که تمامی سی و دو بیت به عنوان یک شناسه منحصربفرد در نظر گرفته شود (نظیر مدل آدرس دهی flat) ، بخشی از آدرس ، شامل آدرس شبکه و سایر بخش ها به عنوان زیرشبکه و یا هاست (سه سطح) و یا صرفا" آدرس هاست (دو سطح) در نظر گرفته می شود .

آدرس دهی شبکه

آدرس شبکه که به آن شماره شبکه نیز گفته می شود ، بطور منحصربفرد هر شبکه را مشخص می نماید . آدرس شبکه هر ماشین موجود بر روی یک شبکه مشابه ، به عنوان بخشی از آدرس IP آن در نظر گرفته می شود . در آدرس IP:172.16.30.56 ، اعداد ۱۶ . ۱۷۲ آدرس شبکه را مشخص می نماید .
آدرس هاست بطور منحصربفرد هر ماشین موجود بر روی یک شبکه را مشخص می نماید. آدرس هاست می بایست منحصربفرد باشد چراکه این آدرس یک ماشین خاص موجود بر روی یک شبکه را شناسائی می نماید . در نمونه آدرس IP:172.16.30.56 ، اعداد ۵۶ . ۳۰ آدرس هاست را مشخص می نماید .
طراحان اینترنت ، با توجه به اندازه شبکه تصمیم به ایجاد کلاس های مختلف شبکه نموده اند:

- برای تعداد شبکه های اندکی که هاست های فراوانی را شامل می شوند، کلاس A در نظر گرفته شده است.
- برای تعداد شبکه های زیادی که دارای هاست های کمتری می باشند ، کلاس C در نظر گرفته شده است .
- برای شبکه های بین شبکه های بسیار بزرگ و بسیار کوچک ، کلاس B در نظر گرفته شده است .

تقسیم یک آدرس IP به آدرس یک شبکه و گره (هاست) توسط کلاس استفاده شده در شبکه مشخص می گردد . شکل زیر کلاس های مختلف شبکه را نشان می دهد :



شکل یک : کلاس های مختلف شبکه

برای هر آدرسی یک مفهوم به نام SubNet Mask وجود دارد که مشخص کننده شناسه شبکه و میزبان(هاست) است. به ازای تعداد بیتهای شبکه عدد یک و به ازای تعداد بیتهای هاست عدد صفر میگذاریم. در ادامه به بررسی کلاس های مختلف شبکه خواهیم پرداخت .

کلاس A

- در یک آدرس شبکه کلاس A ، اولین بایت به آدرس شبکه اختصاص یافته است و سه بایت باقیمانده برای آدرس گره ها در نظر گرفته شده است .
- فرمت کلاس A به صورت network.host. host. host می باشد .
- به عنوان مثال در آدرس IP: ۴۹,۲۲,۱۰۲,۷۰ ، عدد ۴۹ آدرس شبکه و ۷۰ . ۱۰۲ . ۲۲ آدرس هاست را مشخص می نماید . هر ماشین موجود بر روی این شبکه خاص می بایست دارای آدرس شبکه ۴۹ باشد.
- طول آدرس های شبکه کلاس A صرفا" یک بایت است. بیت اول این بایت رزو شده و از هفت بیت باقیمانده برای آدرس دهی استفاده می گردد . بدین ترتیب ، حداکثر ۱۲۸ شبکه کلاس A را می توان ایجاد نمود (دو به توان هفت) .
- اولین بیت مربوط به اولین بایت در یک آدرس شبکه کلاس A می بایست همواره صفر باشد. این بدان معنی است که یک آدرس کلاس A می بایست بین صفر و ۱۲۷ باشد . با توجه به این که در آدرس های کلاس A صرفا" یک بایت برای آدرس شبکه در نظر گرفته می شود در صورتی که این آدرس را با توجه به محدودیت اشاره شده (مقدار صفر اولین بیت در بایت مربوطه) به صورت ۰XXXXXXX در نظر بگیریم و در ابتدا تمامی هفت بیت باقیمانده را صفر (۰۰۰۰۰۰۰۰) و در مرتبه دوم یک (۰۱۱۱۱۱۱۱) در نظر بگیریم ، محدوده آدرس های شبکه کلاس A مشخص می گردد (بین صفر تا ۱۲۷) .
- آدرس شبکه تمام صفر (۰۰۰۰ ۰۰۰۰) ، برای مسیر پیش فرض رزو شده می باشد . همچنین آدرس ۱۲۷ برای اشکال زدائی رزو شده است و نمی توان از آن استفاده نمود که به آن Loop Back میگوییم. بدین ترتیب ، تعداد واقعی آدرس های شبکه کلاس A معادل ۱۲۶ می باشد (۱۲۶ = ۲ - ۱۲۸) .

هر آدرس کلاس A دارای سه بایت (۲۴ بیت) برای آدرس دهی یک ماشین در شبکه است . این بدان معنی است که به تعداد ۲به توان ۲۴ (معادل ۱۶،۷۷۷،۲۱۶) آدرس وجود خواهد داشت که بطور منحصربفرد برای آدرس دهی هاست ها در هر شبکه کلاس A استفاده می شود . با توجه به این که آدرس های هاست تمام صفر و تمام یک رزو شده می باشند تعداد

واقعی هاست ها برای یک شبکه کلاس A معادل ۱۶،۷۷۷،۲۱۴ (دو به توان ۲۴ منهای دو) می‌باشد. بدین ترتیب می توان تعداد بسیار فراوانی هاست را بر روی یک سگمنت شبکه آدرس دهی و استفاده نمود .

برای استخراج محدوده آدرس های معتبر هاست ها در یک شبکه کلاس A می توان از روش زیر استفاده نمود :

- در صورت صفر کردن تمامی بیت های مربوط به هاست (سه بایت) ، آدرس شبکه مشخص می گردد : ۱۰ . ۰ . ۰ . ۰
- در صورت یک کردن تمامی بیت های مربوط به هاست (سه بایت) ، آدرس broadcast مشخص می گردد : ۱۰ . ۲۵۵ . ۲۵۵ . ۲۵۵

هاست های معتبر ، اعداد بین آدرس شبکه و آدرس broadcast می باشند .
(در مثال فوق از ۱۰ . ۰ . ۰ . ۱ تا ۱۰ . ۲۵۵ . ۲۵۵ . ۲۵۴) . بخاطر داشته باشید در مواردی که سعی در یافتن آدرس های معتبر هاست می نمائید ، بیت های هاست نمی توانند تمام صفر و یا تمام یک باشند .

محدوده آدرس ای پی کلاس A: ۱,۱,۱,۱ تا ۱۲۶,۲۵۴,۲۵۴,۲۵۴

SubNet Mask: ۲۵۵,۰,۰,۰

کلاس B

- در یک آدرس شبکه کلاس B ، دو بایت اول اختصاص به آدرس شبکه دارد و از دو بایت باقیمانده برای آدرس دهی گره استفاده می گردد.
- فرمت آدرس های کلاس B به صورت : network.network. host. host می باشد . به عنوان نمونه آدرس IP:172.16.30.5 ، آدرس شبکه ۱۶ . ۱۷۲ و آدرس گره ۵۶ . ۳۰ است .
- اولین بیت مربوط به اولین بایت می بایست همواره مقدار یک و دومین بیت همواره مقدار صفر را داشته باشد . در صورتی که سایر بیت های باقیمانده در بایت اول را صفر (۱۰۰۰۰۰۰۰) و یا یک (۱۰۱۱۱۱۱۱) در نظر بگیریم محدوده شبکه های کلاس B مشخص می گردد .(بین ۱۲۸ تا ۱۹۱) .
- برای آدرس شبکه دو بایت در نظر گرفته شده است . بدین ترتیب ، دو به توان ۱۶ عدد شناسه منحصربفرد برای آدرس دهی شبکه وجود خواهد داشت ولی با توجه به این که تمامی آدرس های شبکه کلاس B می بایست با ۱ و صفر شروع شوند (دو بیت رزو شده) ، برای آدرس دهی شبکه از ۱۴ بیت باقیمانده استفاده خواهد شد . بنابراین در نهایت دو به توان ۱۴ شناسه منحصر بفرد (۱۶،۳۸۴) برای آدرس دهی شبکه های کلاس B وجود خواهد داشت .
- در آدرس های کلاس B از دو بایت برای آدرس دهی هاست ها استفاده می شود . این بدان معنی است که به تعداد دو به توان ۱۶ منهای دو (تمام صفر و تمام یک) یعنی معادل ۶۵،۵۳۴ گره را می توان برای هر شبکه کلاس B آدرس دهی نمود .

برای استخراج محدوده آدرس های معتبر هاست ها در یک شبکه کلاس B می توان از روش زیر استفاده نمود :

- در صورت صفر کردن تمامی بیت های مربوط به هاست (دو بایت) ، آدرس شبکه مشخص می گردد :
۱۷۲ . ۱۶ . ۰ . ۰
- در صورت یک کردن تمامی بیت های مربوط به هاست (دو بایت) ، آدرس broadcast مشخص می گردد :
۱۷۲ . ۱۶ . ۲۵۵ . ۲۵۵

هاست های معتبر، اعداد بین آدرس شبکه و آدرس broadcast می باشند.
(در مثال فوق از ۱ . ۰ . ۱۶ . ۱۷۲ تا ۲۵۴ . ۲۵۵ . ۱۶ . ۱۷۲)

محدوده آدرس ای پی کلاس B: ۱۲۷,۱,۱,۱ تا ۱۹۱,۲۵۴,۲۵۴,۲۵۴

SubNet Mask: ۲۵۵,۲۵۵,۰,۰

کلاس C

- سه بایت اول آدرس های کلاس C به بخش آدرس شبکه و صرفا" یک بایت باقیمانده به آدرس گره اختصاص می یابد . فرمت آدرس های کلاس C به صورت : network.network.network.host است . به عنوان نمونه در آدرس IP:192.168.100.102 ، آدرس شبکه ۱۰۰ . ۱۶۸ . ۱۹۲ و آدرس گره ۱۰۲ می باشد.
- در شبکه های کلاس C ، دو بیت اولین اکتت یک و سومین بیت همواره صفر است (۱۱۰) . برای مشخص کردن محدوده آدرس های شبکه کلاس C پس از دنبال نمودن فرآیندی مشابه با آنچه که در مورد کلاس A و B اشاره گردید می توان محدوده شبکه های کلاس C را بدست آورد (بین ۱۹۲ تا ۲۲۳) . بنابراین در صورت مشاهده یک آدرس IP که شروع آن با ۱۹۲ تا ۲۲۳ است ، مشخص می گردد که آدرس فوق یک آدرس IP کلاس C می باشد .
- در یک آدرس شبکه کلاس C ، سه بیت اول بایت اول ۱۱۰ می باشد . بدین ترتیب می توان با انجام محاسباتی ساده تعداد شبکه دردسترس کلاس C را مشخص نمود . ۳ بایت (و یا ۲۴ بیت) منهای سه بخش رزو شده ، ۲۱ بیت جهت آدرس دهی را ارائه می نماید که به کمک آنها می توان به تعداد ۲ به توان ۲۱ و یا ۲،۰۹۷،۱۵۲ شبکه کلاس C را ایجاد نمود .
- هر شبکه منحصربفرد کلاس C از یک بایت برای آدرس دهی هاست ها استفاده می نماید . بدین ترتیب به تعداد دو به توان ۸ و یا ۲۵۶ منهای دو آدرس رزو شده (تمام صفر و یا تمام یک) را می توان برای هر شبکه کلاس C آدرس دهی نمود (۲۵۴ هاست) .

برای استخراج محدوده آدرس های معتبر هاست ها در یک شبکه کلاس C می توان از روش زیر استفاده نمود :

- در صورت صفر کردن تمامی بیت های مربوط به هاست (یک بایت) ، آدرس شبکه مشخص می گردد :
۱۹۲ . ۱۶۸ . ۱۰۰ . ۰
- در صورت یک کردن تمامی بیت های مربوط به هاست (یک بایت) ، آدرس broadcast مشخص می گردد:
۱۹۲ . ۱۶۸ . ۱۰۰ . ۲۵۵

هاست های معتبر ، اعداد بین آدرس شبکه و آدرس broadcast می باشند .
(در مثال فوق از ۱ . ۱۰۰ . ۱۶۸ . ۱۹۲ تا ۲۵۴ . ۱۰۰ . ۱۶۸ . ۱۹۲) .

محدوده آدرس ای پی کلاس C: ۱۹۲,۱,۱,۱ تا ۲۲۳,۲۵۴,۲۵۴,۲۵۴

SubNet Mask: ۲۵۵,۲۵۵,۲۵۵,۰

کلاس های D و E

آدرس های بین ۲۲۴ و ۲۵۵ برای شبکه های کلاس D و E رزو شده اند . از کلاس D (بین ۲۲۴ تا ۲۳۹) برای آدرس های multicast و از کلاس E (بین ۲۴۰ تا ۲۵۵) برای اهداف علمی و تحقیقاتی استفاده می گردد .

Super Sub Netting:

وقتی در شبکه ای به تعداد بالایی IP نیاز داشته باشیم میتوان از بیت های هاست به بیت های شبکه قرض داد و شبکه را به چندین زیرشبکه تقسیم کرد. اینکار از طریق Super Sub Netting امکان پذیر است. این مفهوم را با زدن یک مثال توضیح میدهیم:

به فرض IP اختیاری ۱۳۱,۱۰,۰,۰ را داشته باشیم و بخواهیم این IP را به ۴ رنج مختلف تقسیم کنیم. به طور پیش فرض Sub Net Mask کلاس B (۲۵۵,۲۵۵,۰,۰) میباشد.

شکل باینری IP : ۱۰۰۰۰۰۱۱,۰۰۰۰۱۰۱۰,۰۰۰۰۰۰۰۰,۰۰۰۰۰۰۰۰

۳ بیت از سمت چپ اول هاست جدا کرده چون با ۳ بیت میتوان ۴ رنج مختلف را نشان داد.

رنج اول(۰۰۱):

۱۰۰۰۰۰۱۱,۰۰۰۰۱۰۱۰,۰۰۱۰۰۰۰۰,۰۰۰۰۰۰۰۰ =۱۳۱,۱۰,۳۲,۰ تا

۱۰۰۰۰۰۱۱,۰۰۰۰۱۰۱۰,۰۰۱۱۱۱۱۱,۱۱۱۱۱۱۱۱ =۱۳۱,۱۰,۶۳,۲۵۴

رنج دوم(۰۱۰):۱۰۰۰۰۰۱۱,۰۰۰۰۱۰۱۰,۰۱۰۰۰۰۰۰,۰۰۰۰۰۰۰۰= ۱۳۱,۱۰,۶۴,۰ تا ۱۳۱,۱۰,۹۵,۲۵۴

رنج سوم(۰۱۱):۱۳۱,۱۰,۹۶,۰ تا ۱۳۱,۱۰,۱۲۷,۲۵۴

رنج چهارم(۱۰۰):۱۳۱,۱۰,۱۲۸,۰ تا ۱۳۱,۱۰,۱۵۹,۲۵۴

Sub Net Mask این IP در کل:۲۵۴,۲۴۵,۲۲۴,۰

نکته: برای بدست آوردن Sub Net Mask کافی است بیت های مربوط به شبکه و ۳ بیتی که به زیرشبکه اختصاص دادیم را یک قرار دهیم و بیت های قسمت هاست را صفر بگذاریم.

پروتکل اینترنت نسخه ۶ (Internet Protocol version 6)

IPv6 جدیدترین نسخه پروتکل اینترنت (Internet Protocol) است که ارتباط‌های اینترنتی بر پایه آن شکل می‌گیرد. این نسخه قرار است جای نسخه ۴ این پروتکل (IPv4) را که هم‌اکنون استفاده می‌شود بگیرد.

IPv4از فضای آدرسی ۳۲ بیتی استفاده می‌کند. این فضا اجازه‌ی آدرس‌دهی $۲^{۳۲}$ یعنی حدود ۴ میلیارد آدرس در اینترنت را می‌دهد. با توجه به این‌که امروزه بسیاری از دستگاه‌ها افزون بر کامپیوترها مانند موبایل‌ها، دوربین‌ها و حتی لوازم خانگی و قاب عکس‌های دیجیتال به اینترنت متصل می‌شوند، این فضا رو به اتمام است و تاکنون با تمهیداتی مانندNATسعی در جبران این کمبود داشته اند. اما IPv6 از فضای آدرس‌دهی ۱۲۸ بیتی استفاده می‌کند که اجازه داشتن $۲^{۱۲۸}$آدرس یگانه را به ما می‌دهد و مشکل فضای آدرسی که هم‌اکنون با آن روبرو هستیم را رفع می‌کند.

امنیت یکی از مشخصات داخلی پروتکل IPv6 است که دارای هر دو مشخصه تصدیق هویت (Authentication)و رمزنگاری (Encryption)در لایه IP پروتکل جدید است. IETFسازمانی است که به گروه کاری امنیت در IP معروف است. این سازمان وظیفه دارد که مکانیزمهای امنیتی مورد نیاز در لایه‌های مختلف IP را هم در IPv6 و هم در IPv4 جهت گسترش و بهبود استانداردهای مورد نیاز بر عهده گیرد. همچنین این گروه وظیفه دارد پروتکل‌های مدیریتی کلید عمومی (Key Management Protocols)را جهت استفاده بیشتر در شبکه جهانی اینترنت توسعه و گسترش دهد. تصدیق (Authentication)این قابلیت را به گیرنده بسته می‌دهد که مطمئن شود آدرس مبدا معتبر بوده و بسته در طول زمان انتقال دچار تغییر و دستکاری نخواهد شد. رمز نگاری (Encryption)اطمینان می‌بخشد که تنها گیرنده اصلی بسته می‌تواند به محتویات آن دست یابد. به عبارت دیگر رمز نگاری باعث می‌شود که تنها گیرنده‌ای که بسته به نام او ارسال شده‌است، می‌تواند به محتویات آن دسترسی داشته باشد. برای بررسی و تحلیل این مزایا یک سیستم کلیدی بکار گرفته می‌شود که به موجب آن فرستنده‌ها و گیرنده‌ها بر روی یک مقدار کلیدی که مورد استفاده قرار می‌گیرد با هم به توافق می‌رسند. سیستم مدیریت کلید عمومی که توسط طراحان IPv6 پذیرفته شده‌است، مکانیزم ISAKMP می‌باشد، که با ایجاد و تولید کلید رمز سر و کار دارد و روشهای اجرای عمومی پروتکل مدیریت کلید را تامین می‌کند. پیغامهایISAKMP با استفاده از پروتکل UDP رد و بدل می‌شوند و از شماره پورت ۵۰۰ استفاده می‌کند .

IPv6الزوم IPSEC را اجباری می‌کند و در نتیجه یک قالب امنیتی یک پارچه برای ارتباطات اینترنتی ایجاد می‌کند IPSEC .برای پیاده‌سازی رمزنگاری و نیز تصدیق استفاده می‌شود. در بسیاری از پیاده‌سازی‌های IPv4 امکان فعال سازی IPSEC نمی‌باشد و در نتیجه سطح امنیت کاهش می‌یابد.

ویژگی هایIPv6

۱) فضای آدرس بزرگتر

۲) پیکربندی خودکار آدرس به وسیله ی Stateless

۳) Multicast

۴) امنیت الزامی لایه ی شبکه (Mandatory Network Layer Security)

۵) ساده تر شدن پردازش توسط روتر ها (Simplified Processing by Routers)

۶) Mobility

۷) Option Extensibility

۸) Jumbo grams

۱) فضای آدرس بزرگتر

یکی از بزرگترین مزیت های این نسخه،مقدار فضای بزرگتر است که قابل قیاس با نسخه ی چهارم نیست . به دلیل همین فضای بزرگ، طراحان IPv6ابنا را بر تقسیم بندی جغرافیایی آدرس ها قرار ندادند . در این نسخه اندازه ی Subnet Mask برابر با (2^{64}) است. یعنی دو برابر کل آدرس های آی پی کنونی !!!! و این یعنی بسیار بعید است تا از تمامی آدرس های این نسخه استفاده شود.ضمن اینکه بزرگی این فضا و ساختار سلسله مراتبی آن، باعث سهولت در مدیریت نیز خواهد شد.

۲) پیکر بندی خودکار (Stateless)

هنگامی که یک دستگاه را به شبکه ی آدرس دهی شده با IPv6متصل می کنیم، خودش به صورت خودکار پیکربندی های لازم را انجام می دهد.برای این کار، میزبان یک درخواست Link-Local Multicast در شبکه ارسال می کند و اگر پیکربندی شبکه صحیح باشد، روتر یک بسته با نام Router Advertisementبه میزبان ارسال می کند که شامل تنظیمات لازم برای پیکربندی است .اگر این آدرس های Classlessبرای نرم افزاری قابل فهم نبود، IPv6همچنان می تواند از DHCPتنظیمات لازم را دریافت کند(State Full)و یا اینکه به صورت دستی کانفیگ شود.

۳) Multicast

بر خلاف IPv4،IPv6از Broadcastبه هیچ عنوان استفاده نمی کند. البته تکنیک مشابه Broadcastدر IPv6زمانی رخ می دهد که یک بسته، به تمامی گره های گروه Multicastارسال شود.

۴) امنیت الزامی لایه ی شبکه (Mandatory Network Layer Security)

استفاده از IPsecکه یک پروتکل رمزگزاری و احراز هویت است، بر خلاف IPv4، در نسخه ی ششم به صورت اجباری مورد استفاده قرار میگیرد. البته بحث در مورد پروتکل های دیگر IPsecبسیار طولانی است.

۵) ساده تر شدن پردازش توسط روتر ها (Simplified Processing by Routers)

این مورد، به دلیل تغییر در ساختار Headerبسته ها در IPv6است.

۶) Mobility

نسخه ی موبایل نسخه ی ششم پروتکل اینترنت (MIPv6)نیز دارای ویژگی های مناسبی برای گره های متحرک است که خارج از بحث ما است.

۷) Option Extensibility

این فضا به راحتی به سرویس هایی مانند Mobilityاجازه می دهند در همین فضا بدون تغییر، توسعه پیدا کنند. بر خلاف IPv4که محدود به ۴۰ بیت بودیم، در این نسخه محدودیت ما اندازه ی کل بسته است.

۸) Jumbo grams

IPv4بسته ها را به بار مفید (Payload) ۴۶کیلوبایتی محدود می کند. اما نسخه ششم مقدار بالاتر از این را هم تا سقف ۴گیگ پشتیبانی می کند که از آن به عنوان Jumbo gramsیاد می شود. این ویژگی باعث افزایش بازدهی شبکه هایی که از MTU استفاده می کنند، می شود.

انواع آدرس دهی درIPv6

۱) Unicast

۲) Multicast

۳) Anycast

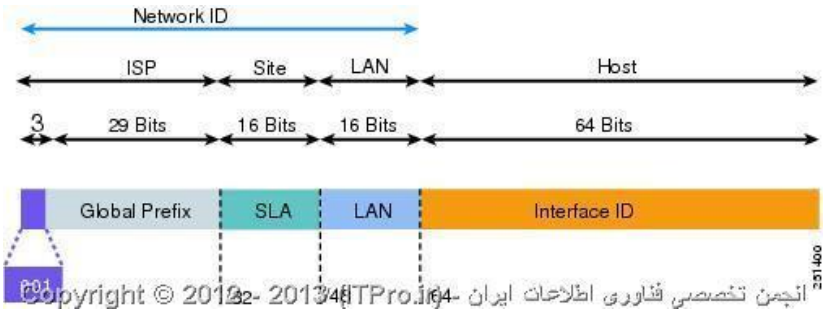
۱) چند نوع مختلف آدرس دهیUnicast

۱. Global Unicast

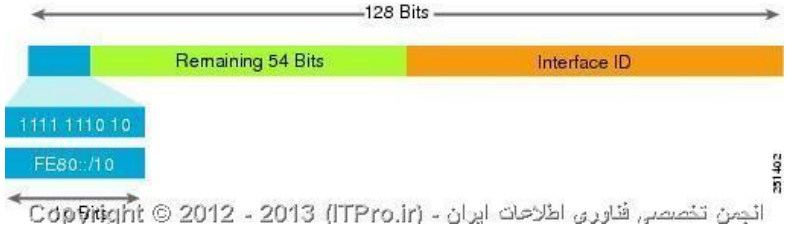
۲. Link-Local Unicast

۳. Unique-Local Unicast

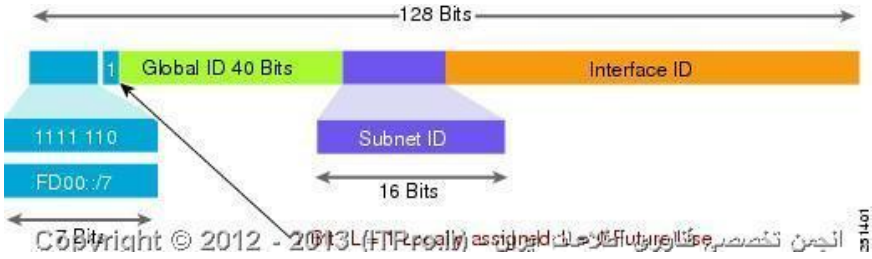
۱. Global Unicastبه مفهوم آدرسهای unicast قابل انتقال در اینترنت بوده (قابلیت آدرس دهی در اینترنت را بر عهده دارند) و شبیه به نوع متناظر آن در IPv4 می باشند ، به این نوع آدرسها Aggregatable Addressنیز می گویند.این ساختار از قسمتهای زیر تشکیل شده است:



۲. Link-Local Unicastشبیه به آدرسهای Private یا خصوصی در IPv4 بوده و قابل انتقال در اینترنت نیستند. این آدرسها را می توان به اعضای یک شبکه LAN و یا چند LAN مختلف که قصد برقراری ارتباط با یکدیگر دارند را تخصیص داد.این آدرسها که در غیاب DHCP Server ایجاد می شوند، در IPv6 معادل Fe80::/64 هستند. به بیانی دیگر اگر در هنگام تنظیم IP آدرس ، در کادر محاوره ای Propertiesکارت شبکه گزینه obtain IPv6 address automaticallyرا انتخاب کنیم، سیستم عامل به طور خودکار براساس تلفیقی از MAC Address مربوط به کارت شبکه با آدرس Link-Local یک آدرس IPv6 به کارت شبکه اختصاص می دهد.

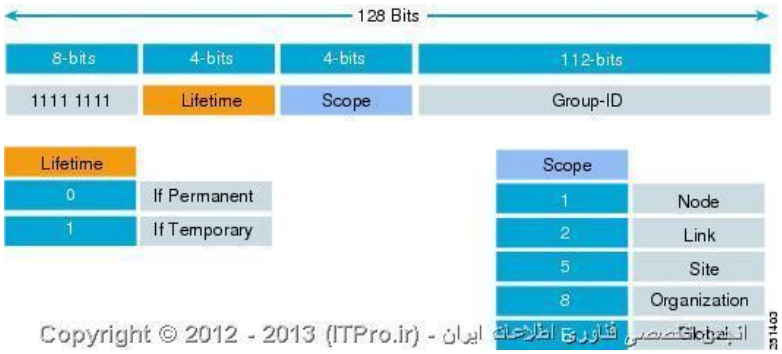


۳. Unique-Local Unicastاین آدرسها را با نام Site-Local unicastهم می شناسند. نیز قابلیت انتقال در اینترنت را نداشته اما در هر جا که مورد استفاده قرار گیرند ، در بین تمامی دیگر آدرسهای اینترنت منحصر به فرد می باشند. عملکرد این نوع آدرسها دقیقا شبیه به آدرسهای private در IPv4 بوده و امکان برقراری ارتباط بین دستگاههای یک سازمان محلی را با واسطه روترها ممکن می سازند.این آدرسها با ۱۶ بیت ثابت (feco) شروع می شوند و به دنبال آن ۳۲ بیت صفر و سپس ۱۶ بیت مربوط به Subnet ID است که معمولا آن را هم صفر در نظر می گیرند.۶۴ بیت پایانی هم که Interface ID است که برای هر کامپیوتر منحصر به فرد است.



۲) آدرسهای Multicast

شبیه بهIPv4 ، پیامهای ارسال شده به مقصد این آدرسها، توسط گروهی از دستگاههای دارای آدرس مزبور دریافت می شود. این آدرسها در برخی از مواقع با نام One-to-Manyنیز نامیده می شوند. در IPv6 آدرسهایی که با FFشروع می شوند، در گروه آدرسهای multicast قرار خواهند گرفت.



۳) آدرس های Anycast

در ارتباط با آدرسهای Anycast برای ساختن یک آدرس Anycast و اختصاص دادن آن به یک router باید ابتدا بخش NET IDمربوط به IPv6 Address شبکه را ثابت و قسمت Subnet ID را صفر قرار دهیم.در واقع می توان گفت که برای ساخت چنین آدرسی نیاز به داشتن IP Prefix شبکه داریم.به طور مثال برای شبکه ۶۴/::۲۰۰۱:۴۱۸۸:۱:۱ آدرس Anycast برابر با ۲۰۰۱:۴۱۸۸:۱:۱:۰:۰:۰:۰ یا در حالت فشرده ::۲۰۰۱:۴۱۸۸:۱:۱ خواهد بود.حال اگر بسته ای به آدرس Anycast ارسال شود ، به دست نزدیکترین آدرسAnycast ی که روی روتر تنظیم شده است می رسد.این عمل با استفاده از ساختارهای مسیریابی آدرسهای Anycastو Routing Metric های مسیریابی اتفاق می افتد و زمانیکه یک packet با آدرس Anycast ارسال شود بعد از اینکه به دست اولین و نزدیکترین دستگاه برسد، دیگر به دنبال دستگاههای دیگر نمی گردد و مسیریابی به اتمام می رسد.

Access Point

Access Point یا Wireless Access Point که به فارسی به معنی نقطه دسترسی می باشد در واقع اسمی است که ما بر روی یکی از تجهیزاتی گذاشته ایم که در شبکه های بیسیم یا وایرلس مورد استفاده قرار می گیرد. این تجهیزات که به صورت اختصاری به آنها AP یا WAP هم گفته می شود در شبکه های کامپیوتری به تجهیزاتی گفته می شود که عملکردی شبیه به سویچ شبکه های کابلی در شبکه های بیسیم دارند ، بدین معنی که این امکان را فراهم می کنند که از طریق آنها شما بتوانید چندین سیستم کامپیوتری را از طریق شبکه های بیسیم به همدیگر متصل کنید. به شبکه های محلی که با استفاده از Access Point ها به هم متصل می شوند به جای اینکه LAN بگوییم Wireless LAN یا WLAN هم می گوییم . Access Point ها را معمولا به شکل AP نمایش می دهند ، این دستگاه ها یک عملکرد مرکزی دارند ، تمامی سیگنال های رادیویی را دریافت و ارسال می کنند که در اکثر مواردی که در شبکه های کامپیوتری می باشد سیگنال های Wi-Fi نیز شامل می شود. معمولا از AP ها در شبکه های کوچک و یا شبکه های عمومی اینترنتی برای ایجاد Hot Spot استفاده می شود .

احتمالا شما نیز در خانه خود از این AP ها دارید ، دستگاهی که شما به عنوان مودم ADSL می شناسید که در کنار آن یک آنتن نیز قرار دارد در واقع یک AP است که در لفظ فنی به آن Wireless Router گفته می شود . AP هایی که در دفاتر شرکت های کوچک و خانه ها استفاده می شوند معمولا بسیار کوچک هستند و براحتی بر روی چیپ یک کارت شبکه یا رادیو قابل پیاده سازی هستند ، حتی مودم های وایمکسی که شما دارید نیز همان AP های خانگی هستند. فناوری های مورد استفاده در AP های این شبکه ها با توجه به استاندارد بودن آنها یکسان است اما معمولا در شبکه های شرکت های بزرگ از AP هایی با قدرت و سرعت بیشتری استفاده می شود. یک نکته بسیار

مهم در خصوص استفاده از AP این است که این تجهیزات به امواج و نویزها بسیار حساس هستند و یک موتور الکتریکی می تواند امواج آنها را براحتی تضعیف کند ، از طرفی وجود مانعی مانند دیوار در یک AP خانگی تا ۳۰ درصد می تواند توان AP شما را کاهش دهد .

Access Point را شما می توانید در همه جا مشاهده کنید از تجهیزات مخابراتی گرفته تا شبکه های کامپیوتری ، در واقع همین دکل هایی که همراه اول یا ایرانسل در شهر دارد به نوعی AP هستند برای دستگاه های وایرلسی که از شبکه تلفن موبایل استفاده می کنند. در شبکه های کامپیوتری از AP ها هم برای استفاده از اینترنت استفاده می شود و هم برای استفاده از شبکه های داخلی ، هیچ محدودیتی در این مورد وجود ندارد. استفاده از تجهیزات وایرلس از جمله همین AP ها امنیت را ناخواسته پایین می آورد ، به قول کارشناسان امنیت اطلاعات ، در شبکه های بیسیم شما هر اندازه که اطلاعات را امن کنید باز هم به اندازه شبکه های کابلی امنیت نخواهید داشت زیرا سیگنال شبکه های بیسیم در همه جا یافت می شود . این خود به نشتی اطلاعات معروف است. توجه کنید که AP ها در همه شبکه های بیسیم از جمله شبکه های تلفن همراه و حتی شبکه های Bluetooth هم استفاده می شوند .

Access Point ها می توانند سیگنال یا بهتر بگوییم امواج رادیویی را تا فاصله معینی ارسال و دریافت کنند و از این بابت دارای محدودیت هستند ، برخی از AP را می توان به گونه ای پیکربندی کرد که در نقش تقویت کننده امواج برای استفاده دورتر از امواج مورد استفاده قرار fبگیرند، به این حالت در اصطلاح Repeater Mode گفته می شود AP .ها می توانند در فرکانس های مختلفی فعالیت کنند که در استانداردهای بین المللی بصورت استاندارد ۸۰۲,۱۱ شناسایی می شوند. پشت دستگاه AP شما همیشه نوع استاندارد ذکر شده است تا بتوانید آن را با دستگاه هایی که از آن استفاده می کنند تطبیق بدهید ، توجه کنید که AP ها فایروال نیستند و به هیچ عنوان فعالیت امنیتی برای حفاظت از شبکه شما انجام نمی دهند بلکه خودشان به تنهایی خطری بزرگ برای شبکه به حساب می آیند. توجه کنید یکی از مواردی که نقطه ضعف شبکه های AP ای می باشد شیوه ارسال و دریافت اطلاعات می باشد که در شبکه های کابلی بصورت دو طرفه همزمان یا Full Duplexاست و در شبکه های بیسیم AP ای بصورت دو طرفه غیر همزمان یا Half Duplex می باشد که خود می تواند عاملی برای کندی شبکه های بیسیم باشد.

Switch

سوئیچ شبکه از مجموعه ای کامپیوتر (گره) که توسط یک محیط انتقال (کابلی یا بدون کابل) به یکدیگر 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 کاربر قادر به 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.

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 به صورت 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 به وجود 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 به دلیل قیمت بالای سوئیچ ، صرفا از سوئیچ به تنهائی استفاده نمی نمایند. در این نوع شبکه ها از ترکیب هاب و سوئیچ استفاده می گردد. مثلا یک سازمان می تواند از چندین هاب به منظور اتصال کامپیوترهای موجود در هر یک از دپارتمانهای خود استفاده و در ادامه با استفاده از یک سوئیچ تمام هاب ها(مربوط به هر یک از دپارتمانها) به یکدیگر متصل می گردد.

روتر

استفاده از روترها در شبکه به امری متداول تبدیل شده است . یکی از دلایل مهم گسترش استفاده از روتر ، ضرورت اتصال یک شبکه به چندین شبکه دیگر اینترنت و یا سایر سایت ها ی از راه دور در عصر حاضر است . نام در نظر گرفته شده برای روترها ، متناسب با کاری است که آنان انجام می دهند : " ارسال داده از یک شبکه به شبکه ای دیگر " . مثلا" در صورتی که یک شرکت دارای شعبه ای در تهران و یک دفتر دیگر در اهواز باشد ، به منظور اتصال آنان به یکدیگر می توان از یک خط leased اختصاصی که به هر یک از روترهای موجود در دفاتر متصل می گردد ، استفاده نمود . بدین ترتیب ، هر گونه ترافیکی که لازم است از یک سایت به سایت دیگر انجام شود از طریق روتر محقق شده و تمامی ترافیک های غیرضروری دیگر فیلتر و در پهنای باند و هزینه های مربوطه ، صرفه جوئی می گردد .

روترهای سخت افزاری : روترهای فوق ، سخت افزارهائی می باشند که نرم افزارهای خاص تولید شده توسط تولید کنندگان را اجراء می نمایند در حال حاضر صرفا" به صورت black box به آنان نگاه می کنیم .نرم افزار فوق ، قابلیت روتینگ را برای روترها فراهم نموده تا آنان مهمترین و شاید ساده ترین وظیفه خود که ارسال داده از یک شبکه به شبکه دیگر است را بخوبی انجام دهند . اکثر شرکت ها ترجیح می دهند که از روترهای سخت افزاری استفاده نمایند چراکه آنان در مقایسه با روترهای نرم افزاری، دارای سرعت و اعتماد پذیری بیشتری می باشند . شکل زیر یک نمونه روتر را نشان می دهد.

روترهای نرم افزاری : روترهای نرم افزاری دارای عملکردی مشابه با روترهای سخت افزاری بوده و مسئولیت اصلی آنان نیز ارسال داده از یک شبکه به شبکه دیگر است. یک روتر نرم افزاری می تواند یک سرویس دهنده NT ، یک سرویس دهنده نت ور و یا یک سرویس دهنده لینوکس باشد . تمامی سیستم های عامل شبکه ای مطرح ،دارای قابلیت های روتینگ از قبل تعبیه شده می باشند .

در اکثر موارد از روترها به عنوان فایروال و یا gateway اینترنت ، استفاده می گردد . در این رابطه لازم است به یکی از مهمترین تفاوت های موجود بین روترهای نرم افزاری و سخت افزاری ، اشاره گردد : در اکثر موارد نمی توان یک روتر نرم افزاری را جایگزین یک روتر سخت افزاری نمود ، چراکه روترهای سخت افزاری دارای سخت افزار لازم و از قبل تعبیه شده ای می باشند که به آنان امکان اتصال به یک لینک خاص

WANاز نوع Frame Relay ، ISDNو یا ATM را خواهد داد .یک روتر نرم افزاری نظیر سرویس دهنده ویندوز دارای تعدادی کارت شبکه است که هر یک از آنان به یک شبکه LAN متصل شده و سایر اتصالات به شبکه های WAN از طریق روترهای سخت افزاری ، انجام خواهد شد.

مهمترین ویژگی های یک روتر:

روترها دستگاههای لایه سوم مدل مرجع OSI می باشند .

روترها مادامیکه برنامه ریزی نگردند ، امکان توزیع داده را نخواهند داشت .

اکثر روترهای مهم دارای سیستم عامل اختصاصی خاص خود می باشند .

روترها از پروتکل های خاصی به منظور مبادله اطلاعات ضروری خود منظور داده نیست ، استفاده می نمایند .

نحوه عملکرد یک روتر در اینترنت : مسیر ایجاد شده برای انجام مبادله اطلاعاتی بین سرویس گیرنده و سرویس دهنده در تمامی مدت زمان انجام تراکش ثابت و یکسان نبوده و متناسب با وضعیت ترافیک موجود و در دسترس بودن مسیر ، تغییر م نماید .

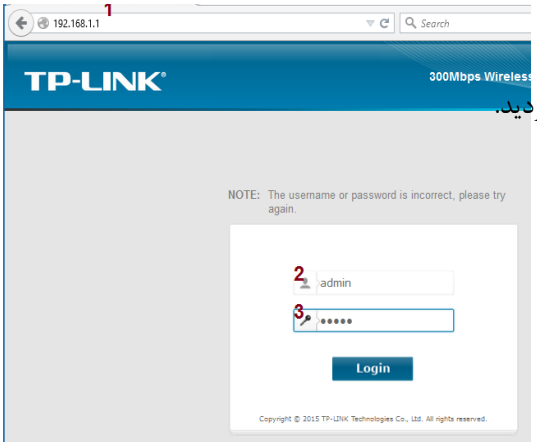
اینترنت یکی از شاهکارهای بشریت در زمینه ارتباطات است . با ایجاد زیر ساخت مناسب ارتباطی ، کاربران موجود در اقصی نقاط دنیا قادر به ارسال نامه های الکترونیکی ، مشاهده صفحات وب ، ارسال و دریافت فایل های اطلاعاتی در کمتر از چند ثانیه می باشند. شبکه ارتباطی موجود با بکارگیری انواع تجهیزات مخابراتی، سخت افزاری 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.

Configure the Modem

کانفیگ کردن مودم

- پیش از آن که به بحث کانفیگ کردن مودم بپردازیم، باید متوجه آدرس Gateway پیشفرض شوید.

Gateway آدرس IP ای است که کامپیوترها به وسیله آن با مودم یا روتر ارتباط برقرار می‌کنند. این آدرس به احتمال اکثرا ۱۹۲,۱۶۸,۱,۱ یا ۱۹۲,۱۶۸,۰,۱ که بر پشت مودم زده شده است.



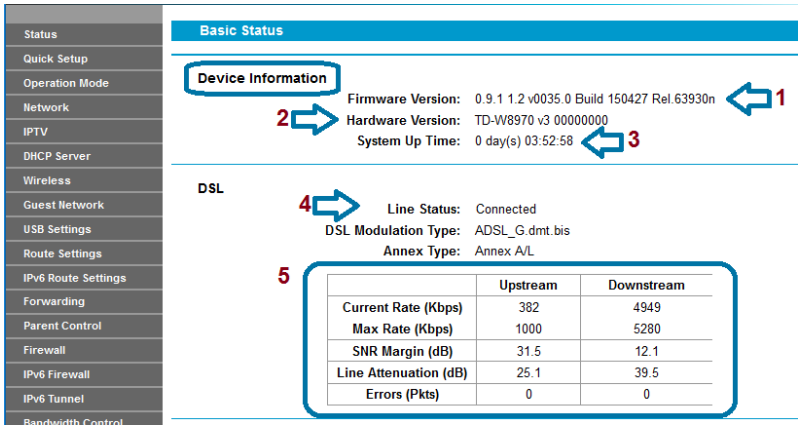
۱. ابتدا مرورگر خود را باز کرده سپس به آدرس Gateway خود بروید.

۲. Username خود را وارد کنید که ان معمولا بر پشت مودم زده شده است و اکثرا admin میباشد.

۳. Password خود را وارد کنید که ان هم معمولا بر پشت مودم زده شده است و اکثرا admin میباشد.

- پس از ورود به تنظیمات در مرحله دوم با صفحه‌ای مشابه تصویر زیر مواجه خواهید شد.

این صفحه نشان دهنده اطلاعات مودم و وضعیت خط شما میباشد.



۱. نشان دهنده نسخه سیستم عامل

۲. نشان دهنده نسخه سخت افزار

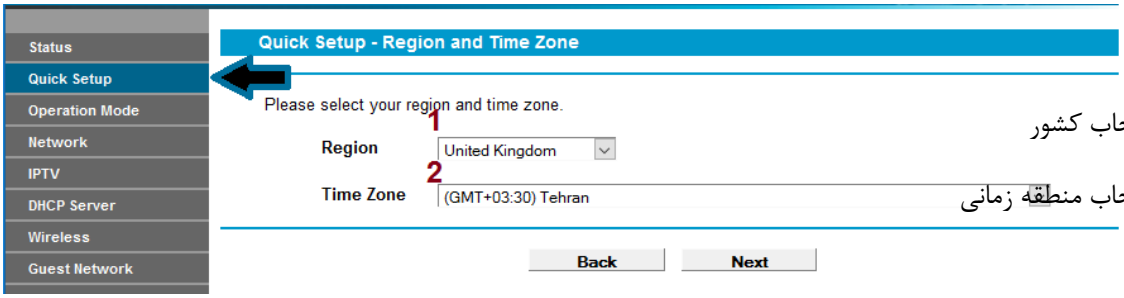
۳. اخرین زمان روشن شدن

۴. وضعیت خط

۵. اطلاعات خط مانند نویز، سرعت انتقال و...

Quick Setup ✓

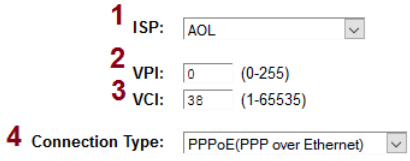
❖ برای کانفیک به صورت Wizard تب Quick Setup را انتخاب میکنیم



۱. انتخاب کشور

۲. انتخاب منطقه زمانی

❖ سپس تنظیمات مربوط به DSL را انجام میدهیم.



۱. ISP شرکتی که شما از ان اینترنت خریده اید می باشد

۲. Virtual Path Identifier

۳. Virtual Circuit Identifier

مقادیر VCI , VPI توسط ISP مشخص می‌شوند و نشان دهنده کانال انتقال داده اند.

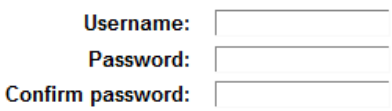
۴. نوع اتصال است که دو نوع ان را شرح میدهیم:

I. Bridging در این حالت باید یک کانکشن روی سیستم عامل خود ساخته و هر بار پس از روشن کردن کامپیوتر خود، برای اتصال به اینترنت تلاش نمایید، درست مثل زمانی که کارت اینترنت خریداری کرده و از Dial-Up استفاده می کنید، مزیت این روش آن است که چنانچه به اینترنت متصل نشوید، یک Error به نمایش در می آید که با استفاده از عددِ Error می توانید مشکل را تشخیص داده و یا با اعلام آن به پشتیبانی فنی، آنها را در تشخیص مشکلتان یاری نمایید!

II. PPPoE در این حالت کانکشن روی مودم ساخته می شود، بنابراین در حین کانفیگ مودم، از شما Username و Password خواسته می شود و دیگر نیازی به ساخت کانکشن روی سیستم عامل وجود نخواهد داشت، مزیت این

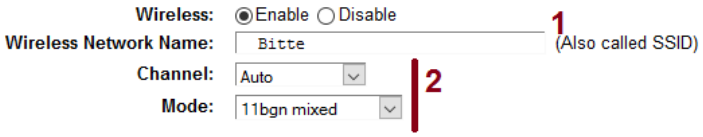
روش آن است که زمانی که کامپیوتر خود را روشن می کنید، به اینترنت متصل هستید، معمولا در جایی که بیش از یک کامپیوتر قرار داشته و یا از مودم Wireless استفاده می شود، از این روش بهره می برند.

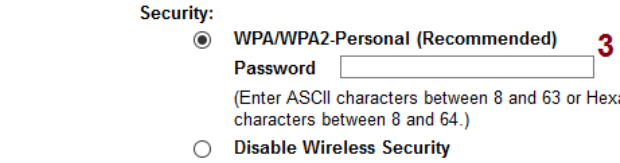
❖ پس از انتخاب PPPoE از ما Username , Password خواسته میشود



که این را هم ISP به ما میدهد

❖ سپس به تنظیمات وایرلس میرسیم.





۱. نام دلخواه وایرلس

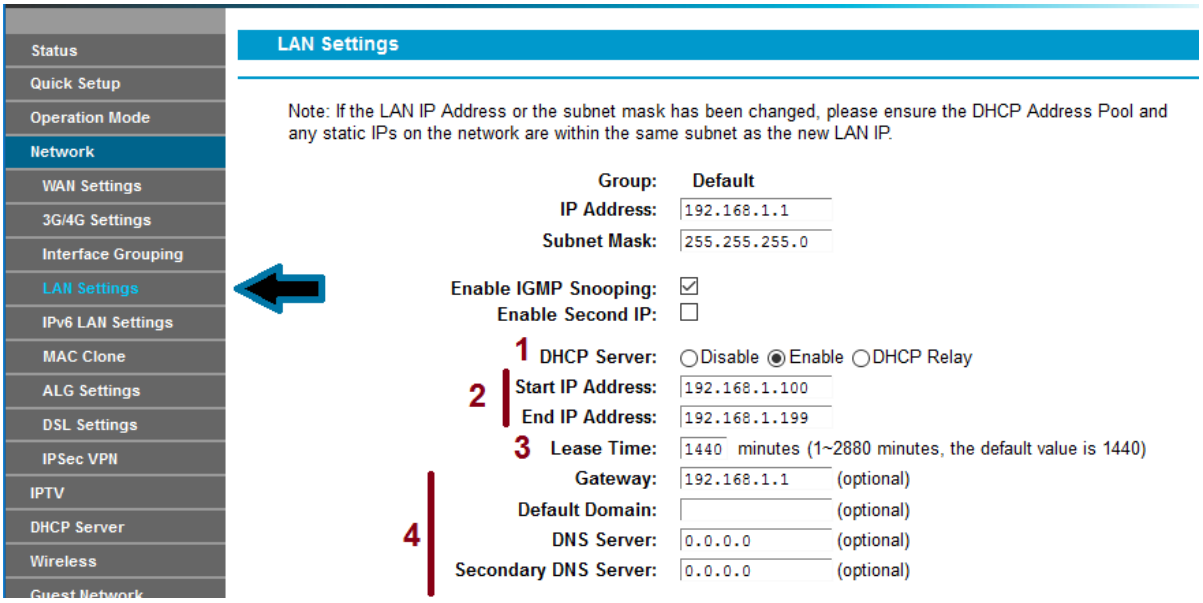
۲. کانال و مد که ISP مشخص میکند

۳. رمز عبور وایرلس

❖ تمام!!! حال یک خلاصه ای از تنظیمات انجام شده داریم در صورت تایید مودم تنظیم و reboot میشود.

✓ LAN Configure:

❖ برای تنظیمات پورت های LAN خود به تبNetwork ← LAN setting بروید.



۱. فعال سازی DHCP :

با فعال سازی DHCP مودم به صورت خودکار به دیوایس ها IP میدهد.

۲. تعیین رنج IP های DHCP

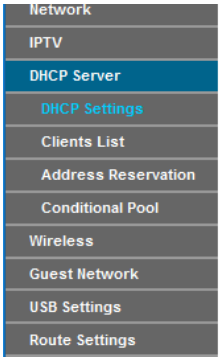
۳. زمان اجاره IP ها :

یعنی پس از اتمام زمان اجاره همه IP ها صفر میشوند و دوباره مودم به هر دیوایس IP میدهد.

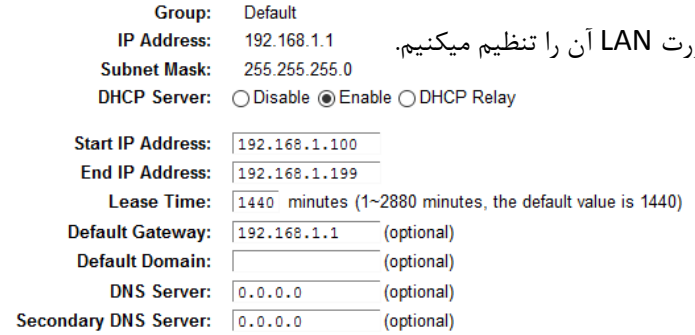
۴. تنظیمات دیگر مانند DNS , Gateway و...

✓ DHCP Configure:

❖ برای تنظیمات DHCP مودم به DHCP Server ← DHCP Setting میرویم.

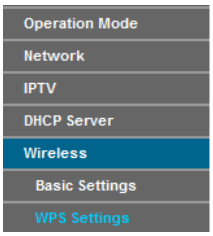


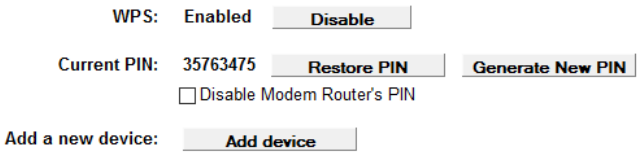
و مانند DHCP پورت LAN آن را تنظیم میکنیم.



✓ WPS:

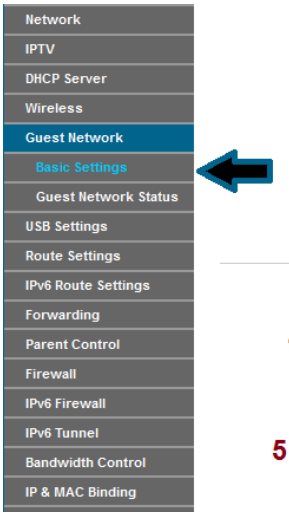
Wi-Fi Simple Config روش ساده برای اتصال دیوایس به مودم است که به جای استفاده از کلمه عبور در زمان اتصال دیوایس به مودم دکمه WPS را فشار میدهیم و دیوایس به مودم بدون کلمه عبور متصل میشود.

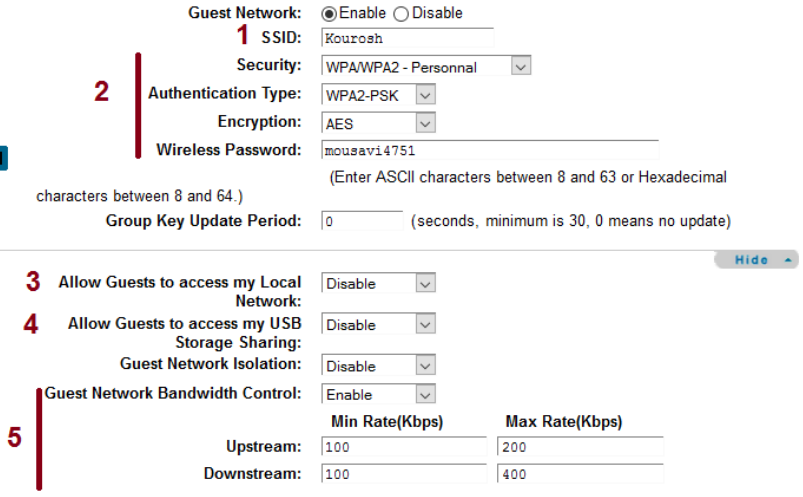




✓ Guest Network:

در برخی از مودم ها شبکه مهمان وجود دارد که میتوان شبکه دیگری ساخت و آن را کنترل کرد





۱. نام شبکه

۲. تنظیمات رمز عبور

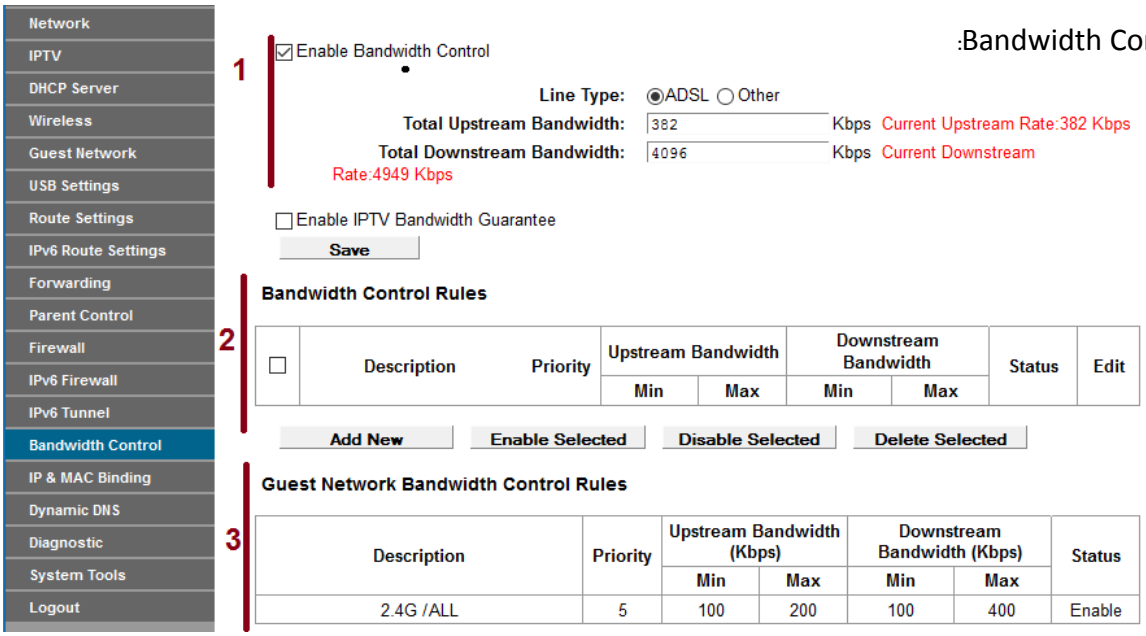
۳. دسترسی به شبکه محلی

۴. دسترسی به USB

۵. تنظیمات محدودیت پهنای باند

پنجمی برای ما ایرانیاس ویژه مهمان ☺

✓ Bandwidth Control:

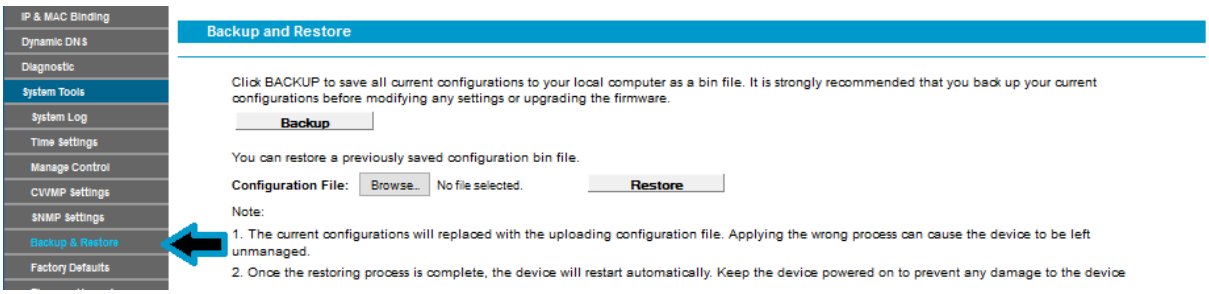


۱. فعالسازی کنترل پهنای باند اصلی و محدودیت آن بر روی تمام مودم(...-LAN –WiFi –Guest)

۲. نوشتن قانون هایی برای کنترل پهنای باند مانند اینکه بگوییم این IP پهنای باندش ۴۰۹۶ باشد و دیگری ۱۰۲۴

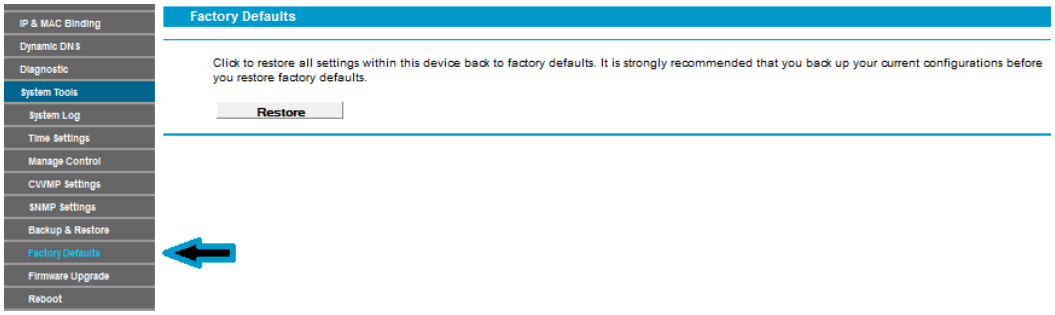
۳. نوشتن قانون هایی برای کنترل پهنای باند شبکه مهمان که همانند کنترل پهنای باند اصلی میباشد.

✓ Backup And Restore:



پس از انجام تنظیمات مودم میتوانید از ان بکاپ گرفته و در صورت بروز مشکل دوباره کانفیگ را انجام ندهید و آن را Restore کنید

✓ Reset Factory:



در صورتی که خواستید مودم را به حالت کارخانه بازگردانید باید به منوی System Tools ← factory Default رفته و Restore را زده تا مودم ریست شود.

تجهیزات امنیت شبکه

امنیت شبکه IDSوIPS

داخلی اشاره دارد. WAN و LANسطح شبکه در مدل امنیت لایه بندی شده به شبکه داخلی ممکن است شامل چند کامپیوتر و سرور و یا پیچیده تر یعنی شامل اتصالات نقطه به نقطه به دفترهای کار دور باشد. بیشتر شبکه های امروزی در ورای پیرامون، باز هستند؛ یعنی هنگامی که داخل شبکه قرار دارید، می توانید به راحتی در میان شبکه حرکت کنید که به این ترتیب این شبکه ها برای هکرها و افراد بداندیش به اهدافی وسوسه انگیز مبدل می شوند. تکنولوژی های ذیل امنیت را در سطح شبکه برقرار می کنند.

بنابه نیازی که داریم موارد مورد نیاز را تیک می زنیم و بر روی Next کلیک می کنیم.

برای Rule ی که ایجاد کرده ایم یک نام اختصاص می دهیم و اگر نیاز بود توضیحاتی را در فیلد دوم وارد می کنیم و کلید Finish را فشار می دهیم.

دستورات پر کاربرد شبکه Cmd

در اینجا به معرفی برخی دستورات شبکه می پردازیم . برای اجرای این دستوران باید از محیط command prompt استفاده کنید .

طریقه ی ایجاد این محیط به این شکل است که در منوی ویندوز ، در قسمت سرچ ، عبارت cmd را تایپ کرده و سپس کلید enter را فشار دهید .

۱) دستور IPCONFIG :

یکی از دستورات مفید به منظور بررسی وضعیت پیکربندی TCP/IP در کامپیوتر های سرویس دهنده یا سرویس گیرنده ای است که بر روی آنان ویندوز نصب شده است . در یونیکس و لینوکس از دستور

IFCONFIG در این رابطه استفاده می شود .

استفاده از IPCONFIG :

برای استفاده از دستور فوق ، کافیست نام آن را در پنجره COMMAND PROMPT تایپ نمود . عملکرد IPCONFIG و اطلاعاتی که در اثر اجرای آن نمایش داده خواهد شد به نوع سوییچ استفاده شده بستگی دارد.

استفاده از IPCONFIG بدون سوییچ اطلاعات پیکربندی TCP/IP در ارتباط با هریک از آداپتور های موجود بر روی سیستم را نمایش خواهد داد .

IPآدرس

SUBNET MASK

DNSاطلاعات سرویس دهنده

DOMAIN

دستورات فوق اطلاعات مربوط به اتصالات از نوع PPP که از آن در DIALUP و VPN استفاده می شود را نیز نمایش خواهد داد .

استفاده از IPCONFIG به همراه سوئیچ ALL علاوه بر نمایش اطلاعات اشاره شده در بخش قبل ، اطلاعات دیگری را نیز نمایش خواهد داد .

آدرس سخت افزاری کارت شبکه (MAC)
اطلاعات مربوط به DHCP
سایر سوئیچ های دستور IPCONFIG :

با استفاده از دستور IPCONFIG و برخی سوئیچ های آن (RELEASE , RENEW) میتوان اطلاعات مربوط به پیکربندی TCP/IP ارائه شده توسط سرویس دهنده DHCP را که در اختیار یک سرویس گیرنده قرار داده شده است را آزاد و یا آنان را مجددا از سرویس دهنده درخواست نمود فرایند فوق به منظور تشخیص عملکرد صحیح سرویس دهنده ی DHCP در شبکه بسیار مفید و کارساز است .

دستور IPCONFIG دارای سوئیچ های مفید متعددی است که میتوان با استفاده از نوع خواسته خود از آن استفاده کرد .

[release [adapter / : آدرس IP پیکربندی شده توسط DHCP را آزاد می نماید. در صورتی که سوئیچ فوق را به تنهایی و بدون مشخص کردن ADAPTER تایپ نماییم ، پیکربندی IP برای تمامی آداپتور های موجود بر روی کامپیوتر ، آزاد می گردد . در صورتی که قصد آزاد سازی اطلاعات پیکربندی مربوط به یک آداپتور خاص را در نظر داشته باشیم ، می بایست به همراه سوئیچ فوق نام آداپتور نیز مشخص گردد .

[renew [adapter/ : یک آدرس IP را بر اساس اطلاعات جدیدی که از DHCP دریافت می نماید ، پیکربندی مجدد می نماید . در صورتی که سوئیچ فوق را به تنهایی و بدون مشخص کردن ADAPTER تایپ نماییم ، پیکربندی IP تمامی آداپتور های موجود برروی

کامپیوتر مجددا انجام خواهد شد . در صورتی که قصد ایجاد مجدد اطلاعات پیکربندی مربوط به یک آداپتور خاص را داشته باشیم ، می بایست به همراه سوئیچ فوق نام آداپتور نیز مشخص گردد .

flushdn / : حذف محتویات DNS RESOLVER CACHE

registerdn / : REFRESH نمودن تمامی اطلاعات تولید شده توسط DHCP برای آداپتور و رجیستر نمودن اسامی DNS

displaydns / : نمایش محتویات DNS RESOLVER CACHE

showclassid[adapter] / : نمایش تمامی DHCP CLASS ID مجاز برای آداپتور

setclassid [adapter][classidtoset]/ : تغییر DHCP CLASS ID

تشخیص نام آداپتور :

نام آداپتور را میتوان با کلیک راست بر روی NETWORK NEIGHBORHOOD و انتخاب گزینه ی PROPERTIES از طریق پنجره ی NETWORK AND DIALUP CONNECTION مشاهده نمود .

IDS چیست؟ Detection System Intrusion

IDS یک سیستم محافظتی است که خرابکاریهای در حال وقوع روی شبکه را شناسایی می کند.روش کار به این صورت است که با استفاده از تشخیص نفوذ که شامل مراحل جمع آوری اطلاعات ، پویش پورتها ، به دست آوری کنترل کامپیوترها و نهایتا هک کردن می باشد ، می تواند نفوذ خرابکاریها را گزارش و کنترل کند.

IPS چیست ؟ System Intrusion Prevention

سیستم جلوگیری از نفوذ (IPS) یک وسیله امنیتی است که بر فعالیت های یک شبکه و یا یک سیستم نظارت کرده تا رفتارهای ناخواسته یا مخرب را شناسایی کند. در صورت شناسایی این رفتارها، بلافاصله عکس‌العمل نشان داده و از ادامه فعالیت آن‌ها جلوگیری می‌کند. سیستم‌های جلوگیری از نفوذ به سه دسته مبتنی بر میزبان و مبتنی بر شبکه و مبتنی بر برنامه تقسیم می‌شوند.

تفاوت میان IPS و IDS چیست؟

IDS بیشتر شبیه یک دزدگیر عمل میکند. IDS قسمتهایی از شبکه را که به نظر می رسدکسی به آنجا صدمه زده کشف می کند و سپس اخطار می دهد. بدیهی است که این اخطار بعد و یا در حین آسیب به دستگاه صورت می گیرد. اکنون زمان آن رسیده که شما از صدمات، پیش تر جلوگیری نموده و سیستم را اصلاح کنید.

IPS برای جلوگیری از ورود بدون مجوز به شبکه یا سرویس دهنده طراحی شده است و بجای اعلام اخطار مبنی بر اینکه قسمتی از سیستم دچار مشکل شده از صدمه سیستم جلوگیری به عمل می آورد.

IPS نسل جدیدی از فن آوری IDS است. سیستم IDS به توانایی احتیاج دارد نه فقط شناسایی. همچنین باید توانایی مسدود

کردن حملات را داشته باشد. تفاوت IPS باIDS سنتی در این است که IPS یک سد امنیتی دور تا دور شبکه و یا سرویس دهنده می کشد تا صدمه ای به آن وارد نگردد. از دیگر توانایی های IPS بیرون راندن تراکم موجود در شبکه ، قطع و وصل ارتباط شبکه داخلی با شبکه خارجی و کنترل رفت و آمدها به داخل و خارج شبکه است.
به عبارت ساده تر قابلیت کنترل ارتباط و توانایی بازداشتن حمله ای را که در حال وقوع است دارد. در حالی که ممکن است تفاوت میان IPS و IDS گیج کننده به نظر آید از اسامی آنها به سادگی می توان تفاوت میانشان را دریافت. IDS ها بیش از یک دستگاه گردآوری کننده اطلاعات و آگاه کننده اختلالات شبکه نیستند که تنها قادرند هر بسته ای را که قصد عبور دارد ارزیابی و تحلیل کنند. IPS ها تغییر شکل طبیعی IDS ها هستند.
IPS ها دارای همه توانایی های IDS ها هستند ولی در سطحی بالاتر. آنها در حقیقت می توانند بر اساس معیار هایی که به آنها می دهیم تصمیم بگیرند. در نتیجه IPSها، دارای مکانیسم پیشگیری هستند و نه فقط واکنش به یک حمله.

ذاتا تمام IPS ها IDS نیز هستند اما IDS ها IPS نیستند. تفاوت در مکانیزم پاسخ دهی است ، که با تغییر وظایف IDS از حالت انفعالی به حالت تصمیم گیرنده صورت می پذیرد.
هنگامی که مدیر شبکه IPSای را برای بررسی عیوب شبکه فعال می کند IPS بسته های عبوری را بر اساس بانک علائم خود بطور دقیق بررسی می کند. در این میان نه تنها عناوین نامه های الکترونیکی ، بلکه کل محتوای آنها را نیز قبل از ورود به شبکه بررسی می کند و در صورت مخرب بودن ، از ورود آنها جلوگیری به عمل می آورد.

خودکارسازی امنیتی راهی است که منتظر استفاده خرابکاران از یک حفره نمی ماند
کدهای مخرب، ویروس ها و نفوذگران می بایست راهی برای ورود به سیستم پیدا کنند. دیواره های آتش معمولی در جلوگیری از حملات ساده به شبکه ، از طریق پورت های باز یا پرتکل های مختلف موثر بودند. همچنین سیستم های ضد ویروس نیز در شناسایی ویروس هایی که می شناسند و از طریق نامه های الکترونیک و کپی فایل وارد سیستم می شوند، موثر بودند. گرچه نویسنده های کد های مخرب به تازگی استفاده از پروتکل های استاندارد و نقاط ورودی (مانند http و پورت ۸۰) که باید برای انجام کارهای سیستم باز نگه داشته شود را برای نفوذ به داخل سیستم شروع کرده اند.
بدین ترتیب سیستمهای امنیتی که دارای مکانیسم های ثابت هستند به مرور دچار افت عملیاتی میشوند و قادر به پاسخگویی به حملات برنامه ریزی شده پیشرفته نمی باشند. اینجاست که تقش IPSها پر رنگ می گردد تا بطور کاملاً موثری جلوی نفوذگران را بگیرد.

پورتهای متداول و پرکاربرد شبکه

	پروتکل	پورت	TCP\UDP	کاربرد
1	FTAM	80	TCP	مدیریت و دسترسی انتقال فایل
2	FTP	21	TCP /UDP	فایل پروتکل انتقال
3	SMTP	25	TCP/UDP	پروتکل انتقال پستی ساده
4	SNMP	161	UDP	پروتکل مدیریت شبکه ای ساده
5	Telnet	23	TCP/UDP	:پروتکل اینترنت برای برقراری ارتباط با میزبانهای راه دور و پردازش محلی داده
6	NCP			پروتکل هسته مرکزی
7	HTTP	80	TCP/UDP	پروتکلی که برای انتقال ابرمتن و صفحات وب در شبکه بکار می رود
8	BGP	179	TCP	یک پروتکل دروازه خارجی مبتنی بر RFC
9	ARP			:پروتکلی که برای شناسائی آدرس IPیک ایستگاه براساس
10	DHCP	546	TCP /UDP	پروتکلی جهت تخصیص آدرس های IP بصورت پویا است
11	IPX	213	TCP/UDP	رشته پروتکل IPX/SPX شرکت Novell برای تعیین مسیر و ارسال بسته
12	IAX2	4569	UDP	هم بسته های کنترلی ارتباط و هم بسته های دیتا (صوت و تصویر) منتقل می کند.
13	DNS	53	TCP/UDP	DNSیک سیستم سلسه‌مراتبی نام‌گذاری برای کامپیوترها، سرویس‌ها، و یا هر منبع دیگری که به شبکه

اینترنت و یا یک شبکه خصوصی (LAN) متصل بوده، می‌باشد.				
برای انتقال میزان کم اطلاعات	TCP/UDP	24	UDP	14
	TCP/UDP	524	NFS	15
	TCP/UDP	135	RPC	16
	TCP/UDP	401	UPS	17
part of Network News Transfer Protocol	TCP/UDP	443	NNSP	18
Microsoft-DS SMB file sharing	TCP	445	SMB	19
INTERNET PRINTING PROTOCOL	TCP/UDP	631	IPP	20
Hyper Text Coffee Pot Control Protocol	TCP/UDP	80	HTCPCP	21
Media Transfer Protoco	TCP/UDP	57	MTP	23
Secure Hyper Text Transfer Protocol	UDP	443	HTTPS	24
Secure Shell	TCP/UDP	22	SSH	25

.

فایروال

مقدمه

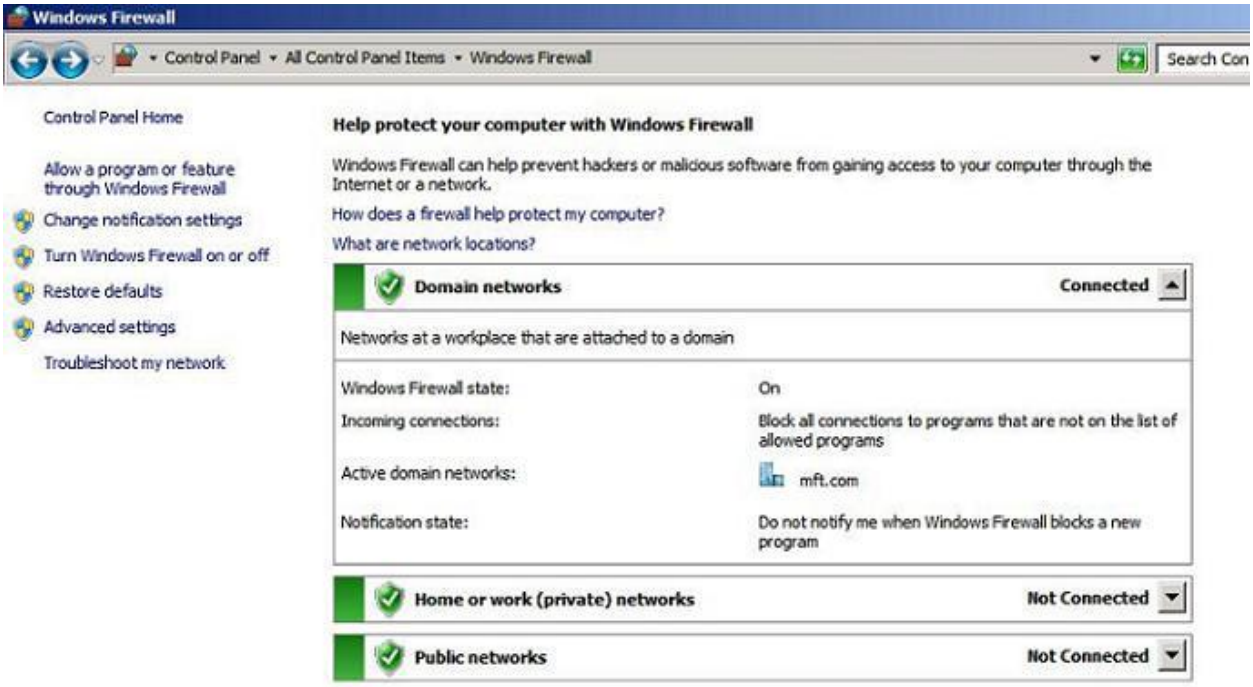
از زمان معرفی اولین فایروال ساخته شده در سیستم عامل ویندوزxp ، شرکت مایکروسافت به طور مداوم در نسخه های بعدی ویندوز، فایروال خود را بهبود بخشیده است. تنظیمات فایروال در سیستم عامل کلاینت یعنی ویندوز ۷ کامل‌تر شده است و برخی از تنظیمات آن باعث شده است که محیطی بهتر و ساده تر را برای کاربر فراهم کند. در این مقاله نگاهی به نرم افزار فایروال در ویندوز 7انداخته و نشان می‌دهیم چگونه آن را با استفاده از سیاست‌های چندگانه فعال در فایروال پیکربندی نمایید.

تحولی در فایروال ویندوز

نرم افزار فایروال در ویندوز xp ساده و ابتدایی بوده و تنها در برابر ترافیک ورودی محافظت می‌کرد، و هرگونه اتصالات ورودی را که توسط کامپیوتر شما مورد استفاده قرار نمی‌گرفتند، مسدود می‌نمود. این فایروال به طور پیش فرض غیرفعال بود .مایکروسافت در بسته سرویس شماره ۲ خود (SP2) این فایروال را به طور پیش فرض فعال کرد و این امکان را برای مدیران شبکه فراهم ساخت تا آن را از طریق سیاست گروهی بر روی کلاینت‌ها فعال سازند .فایروال در ویندوز ویستا بر اساس یک) WFP پلت‌فرم کردن ویندوزها (جدید ساخته شد و توانایی رفع کردن ترافیک خروجی را از طریق کنسول امنیتی پیشرفته MMC به آن اضافه کرد. مایکروسافت در ویندوز ۷، فایروال را به خصوص برای کامپیوترهای قابل حمل با افزودن قابلیت پشتیبانی سیاست‌های چندگانه گروهی فعال در فایروال، بهینه سازی کرد.

معرفی فایروال در ویندوز ۷

همانند ویندوز ویستا، تنظیمات اولیه فایروال در ویندوز ۷ از طریق کنترل پنل قابل دسترسی است. شما همچنین می‌توانید تنظیمات پیشرفته از جمله پیکربندی ***** کردن برای اتصالات خروجی را از طریق کنترل پنل انجام دهید .این در حالی است که این تنظیمات در ویندوز ویستا از طریق ساختن یک کنسول MMCخالی و افزودن یک snap-in به آن صورت می‌گیرد. همانگونه که در شکل ۱ می‌بینید، بر روی گزینه تنظیمات پیشرفته در سمت چپ پنل کلیک کنید.



شکل۱: در ویندوز ۷، شما از طریق کنترل پنل به تنظیمات پیشرفته فایروال دسترسی دارید.

گزینه های بیشتر برای شبکه

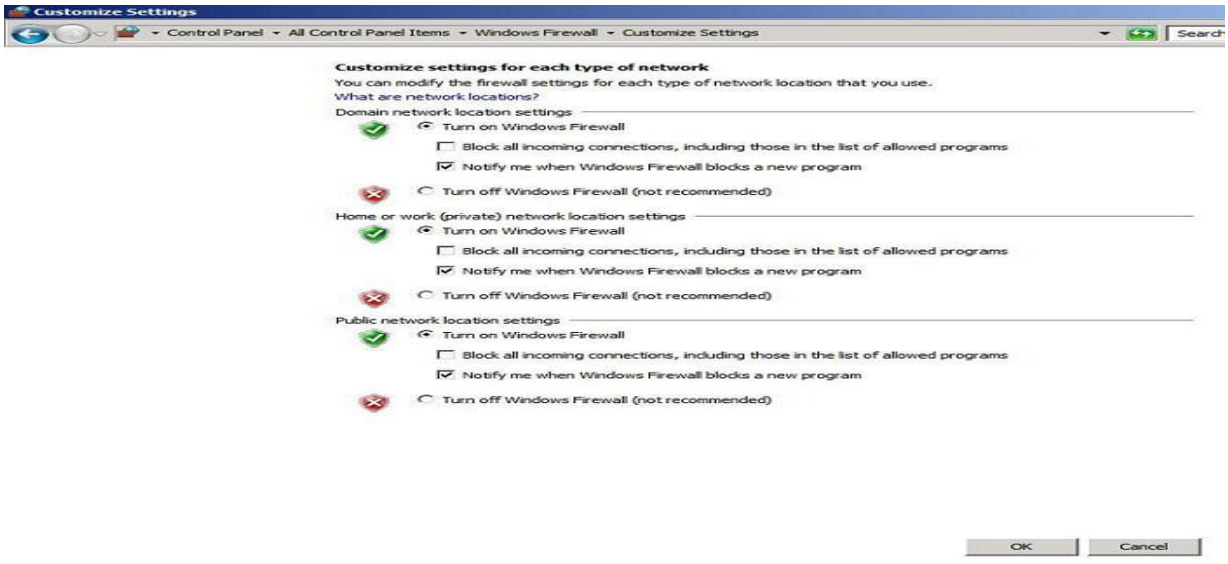
نرم افزار فایروال در ویندوز ویستا به شما این اجازه را می‌دهد که انتخاب کنید که بر روی یک شبکه خصوصی یا عمومی قرار دارید. در ویندوز ۷ شما سه انتخاب شبکه عمومی، شبکه خانگی و شبکه کاری دارید که دو گزینه آخر به عنوان شبکه خصوصی در نظر گرفته شده است.

اگر شما گزینه "شبکه خانگی" را انتخاب کنید، می‌توانید یک homegroup) گروه خانگی) بسازید. در این حالت شناسایی شبکه به طور خودکار فعال می‌شود، در نتیجه شما می‌توانید کامپیوترها و دستگاه‌های دیگری را که روی این شبکه قرار دارند ببینید و آنها هم قادر خواهند بود شما را در این شبکه ببینند. کامپیوترهای متعلق به شبکه خانگی می‌توانند عکس، موسیقی، ویدئو و اسناد موجود در کتابخانه و همچنین دستگاه‌های سخت افزاری مانند پرینتر را با هم به اشتراک بگذارند. اگر پوشه هایی در کتابخانه شما قرار دارند که نمی‌خواهید آنها را با دیگران به اشتراک بگذارید، می‌توانید آنها را از مجموعه اشتراکی خود حذف کنید .

اگر شما گزینه "شبکه کاری" را انتخاب کنید، شناسایی شبکه به طور پیش فرض فعال می‌شود، ولی شما دیگر نمی‌توانید یک گروه خانگی بسازید و عضو آن شوید. اگر شما عضو یک دامنه گردید (از طریق کنترل پنل/سیستم/تنظیمات پیشرفته سیستم/گزینه نام کامپیوتر) و در کنترل کننده دامنه احراز هویت شوید، فایروال به طور خودکار شبکه را به عنوان یک شبکه دامنه تشخیص می‌دهد.

"شبکه عمومی" گزینه مناسبی است برای زمانی که شما به یک شبکه بی‌سیم عمومی در یک فرودگاه، هتل یا کافی شاپ متصل می‌شوید یا از یک شبکه پهن باند استفاده می‌کنید. در این حالت کشف شبکه به طور پیش فرض غیر فعال است، بنابراین کامپیوترهای دیگر این شبکه نمی‌توانند شما را ببینند. همچنین در این حالت قادر نخواهید بود یک homegroup ایجاد کرده یا در آن عضو گردید.

با وجود انواع شبکه، فایروال ویندوز ۷ به طور پیش فرض ارتباط با برنامه هایی که در لیست برنامه های مجاز نمی‌باشند را مسدود می‌کند. ویندوز ۷ به شما اجازه می‌دهد که تنظیمات هر نوع شبکه را به طور مجزا، همانطور که در شکل ۲ می بینید، پیکربندی نمایید.



شکل۲: ویندوز ۷ به شما اجازه می‌دهد که تنظیمات هر نوع شبکه را به طور مجزا پیکربندی کنید.

پروفایل‌های فعال چندگانه

در ویندوز ویستا حتی اگر شما پروفایل‌هایی برای هر دو شبکه عمومی و خصوصی داشته باشید، تنها یکی از آنها اجازه دارد در یک زمان فعال باشد. محدود کننده ترین پروفایل به همه اتصالات اعمال می‌شود، بنابراین شما قادر نخواهید بود هر کاری که در شبکه محلی خصوصی انجام می‌دادید را انجام دهید، زیرا شما تحت نظارت قوانین مربوط به شبکه عمومی هستید.

در ویندوز ۷ و ویندوز سرور R2۲۰۰۸ ، برای هر کارت شبکه پروفایل‌های مجزا می‌تواند فعال شود. اتصالات مربوط به شبکه خصوصی تابع قوانین شبکه خصوصی است، در حالیکه ترافیک‌های به مقصد یا از مقصد عمومی تابع قوانین شبکه عمومی است.

چیزهای کوچکی که به حساب می آیند

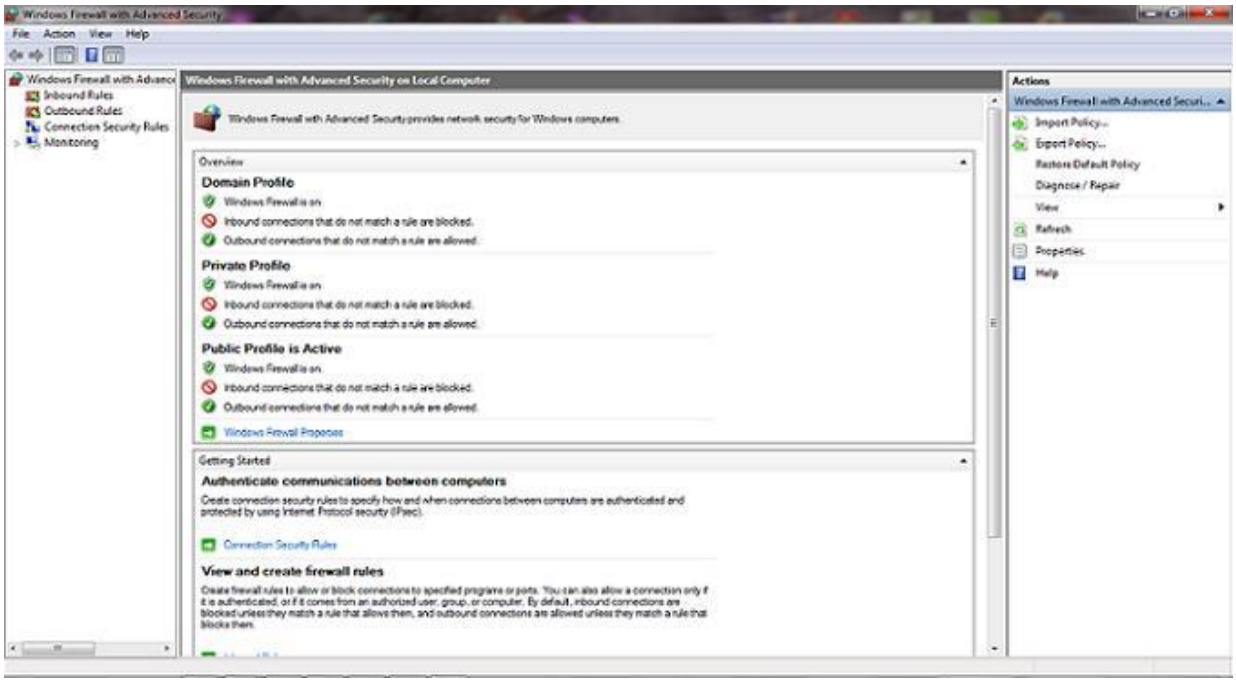
در بسیاری از موارد، قابلیت‌های بیشتر وابسته به تغییرات کوچک است و مایکروسافت با استفاده از نظرات کاربران و تلفیق کردن برخی از آنها، تغییرات کوچکی در فایروال ویندوز ۷ اعمال کرده است. به عنوان مثال، در ویندوز ویستا هنگام ایجاد قوانین فایروال، شما باید به طور مجزا شماره پورت و آدرس IP را ذکر می‌کردید. در صورتیکه در ویندوز ۷ می‌توانید دامنه تغییرات را مشخص کنید که باعث کاهش زمان عملکرد این وظیفه مدیریتی می‌شود.

شما همچنین می‌توانید به جای استفاده از دستورnetsh ، قوانین امنیتی اتصالات را ایجاد کنید و پورت‌ها یا پروتکل‌هایی را به عنوان الزامات IPsec در کنسول فایروال، تعیین کنید .

قوانین امنیتی اتصالات نیز رمزگذاری پویا را پشتیبانی می‌کند. این بدان معنی است که اگر یک سرور یک پیام غیر رمز شده (ولی احراز هویت شده) را از یک کامپیوتر کلاینت دریافت کند، بخش امنیت سرور می‌تواند برای لزوم رمز گذاری به منظور ارتباط امن-تر، با کلاینت مذاکره نماید.

پیکربندی پروفایل‌ها با استفاده از تنظیمات پیشرفته

با استفاده از کنسول تنظیمات پیشرفته، می‌توانید گزینه ها را برای هر یک از انواع پروفایل‌های شبکه، همانطور که در شکل ۳ می-بینید، پیکربندی نمایید.



شکل۳: پیکربندی گزینه ها برای هر پروفایل با استفاده از کنسول تنظیمات پیشرفته

برای هر پروفایل می‌توانید یکی از پیکربندی‌های زیر را داشته باشید:

·وضعیت فعال/غیرفعال فایروال ویندوز

·اتصالات ورودی (مسدود کردن، مسدودکردن همه اتصالات، یا اجازه دادن)

·اتصالات خروجی (اجازه دادن یا مسدود کردن)

·نمایش اطلاعیه (هنگامی که یک برنامه مسدود شده است اطلاع دهد یا اطلاع ندهد)

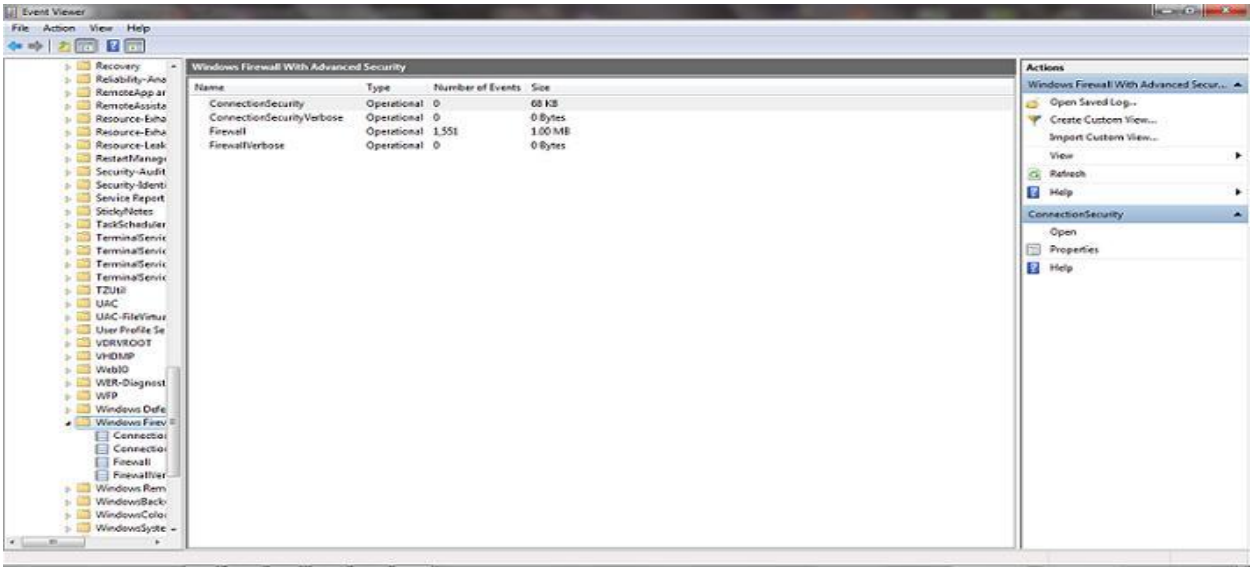
·اجازه پاسخ تکی به ترافیک چند پخشی یا پخشی

·اعمال قوانین محلی فایروال ایجاد شده توسط مدیر محلی علاوه بر قوانین سیاست گروهی فایروال

·اعمال قوانین محلی امنیت ارتباط ایجاد شده توسط مدیران محلی علاوه بر قوانین سیاست گروهی فایروال

ثبت رویداد:

فایروال ویندوز ویستا را می‌توان طوری تنظیم کرد تا رویدادها را در یک فایل که مسیر پیش فرض آن Windows\System32\LogFiles\Firewall\pfirewall.logاست، ثبت نماید. در ویندوز ۷، رویدادها می‌توانند در بخش برنامه ها و سرویس‌ها در پنجره نمایش رویداد (Event Viewer) ثبت شوند که دسترسی به آن ساده تر است. برای دسترسی، پنجره نمایش رویداد را باز کنید و همانطور که در شکل ۴ می بینید، در سمت چپ بر روی گزینه Applications and Services Log | Microsoft | Windows | Windows Firewall with Advanced Security، کلیک کنید



شکل۴: ثبت رویدادهای فایروال ویندوز ۷ در پنجره نمایش رویداد

در بخش ثبت رویدادها در پنجره نمایش رویداد، شما می‌توانید یک نمای سفارشی ایجاد نمایید، فایل ثبت رویداد را باز کنید، در فایل ثبت رویداد جستجو نمایید و غیره.

دستور Netsh

ویندوز ۷ دارای دستور خط فرمان netsh برای فایروال است که این دستور را به منظور سازگاری با نسخه های پیشین قرار داده است. ولی اگر این دستور را اجرا کنید، پیامی با مضمون "مهم، دستور netsh نادرست است. به جای آن از دستور netsh advfirewallاستفاده کنید"، دریافت می‌کنید.

خلاصه

فایروال ویندوز ۷ نسخه بهبود یافته فایروال ویستا است. بسیاری از کاربران ویندوز ویستا، از جمله برخی از متخصصان فناوری اطلاعات، از این مسئله که می‌توانند ترافیک خروجی را ***** کنند و نیز از انجام تنظیمات پیشرفته روی فایروال ویندوز ویستا، بی اطلاع بودند. زیرا هیچ‌یک از این قابلیت‌ها از طریق اپلت فایروال در کنترل پنل قابل مشاهده نیست. مایکروسافت در ویندوز ۷ یک فایروال میزبان تعبیه کرده است که نسبت به پیشینیان خود کاربردی تر است و یک جایگزین مناسب نسبت به محصولات فایروال دیگر شرکت‌ها محسوب می‌شود.

مواردی مضاعف :

۱- اولین گزینه در این محیط (سمت چپ صفحه)، گزینه Allow an app or feature through Windows Firewallمی باشد. این گزینه زمانی به کار میرود که میخواهیم به یک برنامه اجازه ارسال یا دریافت اطلاعات از طریق فایروال را بدهیم. (چه اجازه برای یک نرم افزار و چه باز کردن یک پورت، میتواند برای سیستم شما خطرناک باشد ولی باز کردن یک پورت ، خیلی خطرناک تر از اضافه کردن برنامه به لیست می باشد. چون زمانیکه شما یک پورت را باز می کنید این پورت تا زمانی که خودتان آن را ببندید باز خواهد ماند، ولی اگر یک برنامه را به لیست اضافه کنید، فایروال فقط در مواقع لزوم به برنامه اجازه دریافت و ارسال اطلاعات را می دهد.

۲- دومین گزینه Change notification settings می باشد که پس از ورود به آن می توان نسبت به تنطیم دو مورد زیر بر روی شبکه های محلی و عمومی و یا غیرفعال کردن فایروال قدام کرد.

اولین مورد تمامی ترافیک ورودی را مسدود می کند. حتی ترافیک برنامه هایی را که در گزینه قبل در لیست Allow قرار دادیم.

در مورد دوم نیز به ویندوز اعلام می کنیم، زمانیکه یک برنامه را برای اولین بار بلوک کرد به ما اطلاع دهد.

۳- Turn Windows Firewall on or offنیز دقیقا مشابه گزینه قبل می باشد که از توضیح آن خودداری می کنیم

۴- چهارمین گزینه Restore defaults می باشد که توسط آن تمامی تنظیمات انجام شده برروی فایروال حذف و به حالت اول بر خواهد گشت.

۵- پنجمین گزینه Advanced settings می باشد که عمده تنظیمات فایروال از این گزینه انجام می شود.

در این قسمت می توانیم فیلترهای متعددی در فایروال ویندوز تعریف کنیم. بر حسب اینکه بخواهیم ترافیک ورودی یا خروجی، یک برنامه خاص، یک پورت خاص، اتصال به شبکه های محلی یا عمومی، دامنه خاص یا یک پروتکل خاص را محدود یا آزاد کنیم.

حال برای نمونه میخواهیم جلوی اتصال برنامه kmPlayer را با استفاده از فایروال ویندوز به اینترنت را بگیریم.(از این ترفند میتوان برای جلوگیری از اتصال برنامه ها به اینترنت و جلوگیری از غیرفعال شدن کرک برنامه ها یا جلوگیری از آپدیت شدن برخی از برنامه ها استفاده کرد.)

حال وارد Advanced settings می شویم. در سمت چپ صفحه ای که باز می شود گزینه های متعددی وجود دارد که عمدتا با گزینه های Inbound Rules و Outbound Rules سر و کار خواهیم داشت.

Inbound Rules برای کنترل ترافیک ورودی به سیستم یا شبکه مورد نظر استفاده میشود.

Outbound Rules برای کنترل ترافیک خروجی از سیستم یا شبکه مورد نظر استفاده می شود.
بر روی Outbound Rules کلیک میکنیم. حال در وسط صفحه نمایش، Rule های ایجاد شده توسط ویندوز را مشاهده میکنیم. اگر برنامه ای توسط ما یا توسط ویندوز بلوک شود در این لیست به رنگ قرمز نمایش داده می شود. در سمت راست صفحه نمایش گزینه هایی برای ایجاد Rule جدید یا فیلتر Rule های موجود و یا گزینه هایی برای خروجی گرفتن از وظایف موجود و تنظیمات آنها و همچنین حذف آنها وجود دارد.
برای جلوگیری از اتصال برنامه kmPlayer ابتدا بر روی New Rule کلیک می کنیم. در پنجره باز شده برحسب اینکه چه هدفی داریم از طریق گزینه های موجود در این صفحه می توانیم مسیر خود را ادامه دهیم.
Program :دسترسی های یک برنامه خاص را کنترل می کند.
Port : دسترسی های یک پورت را به پروتکل های TCP و UDP کنترل می کند.
Predefined :استفاده از Rule های از پیش تعریف شده ویندوز.
Custom : پیکربندی Rule بصورت کاملا تخصصی و حرفه ای.
بر روی گزینه Program کلیک می کنیم. در صفحه جدید می توان تمام برنامه های موجود و یا یک برنامه خاص را معرفی کرد. با کلیک بر روی this program path مسیر فایل اجرائی kmPlayer را معرفی می کنیم و برروی NEXT کلیک می کنیم.

در صفحه جدید سه گزینه داریم که عبارتند از :
Allow the connection : این گزینه اجازه ارسال اطلاعات را به برنامه می دهد.
Allow the connection if it secure: در صورتیکه اتصال امن باشد امکان انتقال اطلاعات را می دهد.
Block the connection: کلا اتصال نرم افزار را قطع می کند.

بر روی گزینه سوم کلیک می کنیم.
با ورود به صفحه جدید سه گزینه مشاهده می کنیم که مشخص می کند در هنگام اتصال به کدامیک از موارد ذکر شده این Rule اجرا شود.
Domain: هنگام اتصال به یک دامنه (در صورتیکه سیستم یک ارائه دهنده خدمات باشد).

Private: هنگام اتصال به یک شبکه محلی.

Public: هنگام اتصال به شبکه اینترنت یا شبکه عمومی

بنابه نیازی که داریم موارد مورد نیاز را تیک می زنیم و بر روی Next کلیک می کنیم.
برای Rule ی که ایجاد کرده ایم یک نام اختصاص می دهیم و اگر نیاز بود توضیحاتی را در فیلد دوم وارد می کنیم و کلید Finish را فشار می دهیم.

دستورات پر کاربرد شبکهCMD

در اینجا به معرفی برخی دستورات شبکه می پردازیم . برای اجرای این دستوران باید از محیط command prompt استفاده کنید .

طریقه ی ایجاد این محیط به این شکل است که در منوی ویندوز ، در قسمت سرچ ، عبارت cmd را تایپ کرده و سپس کلید enter را فشار دهید .

۲) دستور IPCONFIG :

یکی از دستورات مفید به منظور بررسی وضعیت پیکربندی TCP/IP در کامپیوتر های سرویس دهنده یا سرویس گیرنده ای است که بر روی آنان ویندوز نصب شده است . در یونیکس و لینوکس از دستور

IFCONFIG در این رابطه استفاده می شود .

استفاده از IPCONFIG :

برای استفاده از دستور فوق ، کافیست نام آن را در پنجره COMMAND PROMPT تایپ نمود . عملکرد IPCONFIG و اطلاعاتی که در اثر اجرای آن نمایش داده خواهد شد به نوع سوییچ استفاده شده بستگی دارد.

استفاده از IPCONFIG بدون سوییچ اطلاعات پیکربندی TCP/IP در ارتباط با هریک از آداپتور های موجود بر روی سیستم را نمایش خواهد داد .

آدرس IP

SUBNET MASK

اطلاعات سرویس دهنده DNS

DOMAIN

دستورات فوق اطلاعات مربوط به اتصالات از نوع PPP که از آن در DIALUP و VPN استفاده می شود را نیز نمایش خواهد داد .

استفاده از IPCONFIG به همراه سوئیچ ALL علاوه بر نمایش اطلاعات اشاره شده در بخش قبل ، اطلاعات دیگری را نیز نمایش خواهد داد .

آدرس سخت افزاری کارت شبکه (MAC)

اطلاعات مربوط به DHCP

سایر سوئیچ های دستور IPCONFIG :

با استفاده از دستور IPCONFIG و برخی سوئیچ های آن (RELEASE , RENEW) میتوان اطلاعات مربوط به پیکربندی TCP/IP ارائه شده توسط سرویس دهنده DHCP را که در اختیار یک سرویس گیرنده قرار داده شده است را آزاد و یا آنان را مجددا از سرویس دهنده درخواست نمود فرایند فوق به منظور تشخیص عملکرد صحیح سرویس دهنده ی DHCP در شبکه بسیار مفید و کارساز است .

دستور IPCONFIG دارای سوئیچ های مفید متعددی است که میتوان با استفاده از نوع خواسته خود از آن استفاده کرد .

[release [adapter] / : آدرس IP پیکربندی شده توسط DHCP را آزاد می نماید. در صورتی که سوئیچ فوق را به تنهایی و بدون مشخص کردن ADAPTER تایپ نماییم ، پیکربندی IP برای تمامی آداپتور های موجود بر روی کامپیوتر ، آزاد می گردد . در صورتی که قصد آزاد سازی اطلاعات پیکربندی مربوط به یک آداپتور خاص را در نظر داشته باشیم ، می بایست به همراه سوئیچ فوق نام آداپتور نیز مشخص گردد .

[renew [adapter/ : یک آدرس IP را بر اساس اطلاعات جدیدی که از DHCP دریافت می نماید ، پیکربندی مجدد می نماید . در صورتی که سوئیچ فوق را به تنهایی و بدون مشخص کردن ADAPTER تایپ نماییم ، پیکربندی IP تمامی آداپتور های موجود برروی کامپیوتر مجددا انجام خواهد شد . در صورتی که قصد ایجاد مجدد اطلاعات پیکربندی مربوط به یک آداپتور خاص را داشته باشیم ، می بایست به همراه سوئیچ فوق نام آداپتور نیز مشخص گردد .

flushdn / : حذف محتویات DNS RESOLVER CACH

registerdn / : REFRESH نمودن تمامی اطلاعات تولید شده توسط DHCP برای آداپتور و رجیستر نمودن اسامی DNS

displaydns / : نمایش محتویات DNS RESOLVER CACHE

showclassid[adapter] / : نمایش تمامی DHCP CLASS ID مجاز برای آداپتور

setclassid [adapter][classidtoset]/ : تغییر DHCP CLASS ID

تشخیص نام آداپتور :

نام آداپتور را میتوان با کلیک راست بر روی NETWORK NEIGHBORHOOD و انتخاب گزینه ی PROPERTIES از طریق پنجره ی NETWORK AND DIALUP CONNECTION مشاهده نمود .

مفهوم DNS CACHE :

زمانی که یک سیستم ، ترجمه (تبدیل نام HOST به آدرس) را از طریق یه سرویس دهنده ی DNS دریافت می نماید .برای مدت زمان کوتاهی آن را در یک CACHE ذخیره مینماید . در صورتی که مجددا از نام استفاده شود ، پشته TCP/IP محتویات CACHE را به منظور یافتن رکورد درخواستی بررسی می نماید .

موارد استفاده از IPCONFIG :

از دستور فوق در مواردی که قصد داریم تشخیص دهیم که آیا سرویس دهنده DHCP و DNS در شبکه به درستی وظایف خود را انجام می دهند ، استفاده می شود .

۳) دستور PING :

PING دستوری است که مشخص می کند آیا یک کامپیوتر خاص که ما IP و یا HOST NAME آن را می دانیم ، روشن و یا فعال هست یا نه ، یا اینکه ما قابلیت اتصال به وی را داریم یا نه ؟

و اینکه اگر فعال باشد ، مدت زمان رسیدن بسته های TCP/IP از آن کامپیوتر به کامپیوتر ما چقدر است .

این دستور دستوری است که هکر های برای خراب کردن SERVER انجام میدن ، اگر کلی کامپیوتر همزمان با هم به یک IP ، PING بدن ، SERVER کل زمانش صرف سرویس دهی به اون

PING ها میشه

کاربرد این دستور به صورت زیر است :

Ping [IP-or-HostName]

که به جای IP یا HOST NAME باید آدرس IP و یا HOSTNAME کامپیوتر مورد نظر را بگذاریم .

در نتایج به دست آمده ، منظور از BYTES مقدار بایت های ارسالی و دریافتی در هر بسته است . منظور از TIME ، مدت زمانی است که طول کشیده تا بسته مورد نظر به مقصد برسد و منظور از TTL ، تعداد گامهای اعتبار بسته ارسالی است .

فرض کنید به یک IP که فعال نیست PING کنیم . نتیجه به صورت زیر خواهد بود :

Pinging 892.868.811.211 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 892.868.811.211:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

که نشان می دهد که آن IP در آن لحظه فعال نیست .

البته تمامی مطالبی که در بالا ذکر شد ، در حالتی است که مستقیما به اینترنت وصل شده اید و یا اگر از طریق شبکه محلی به اینترنت وصل هستید ، شبکه شما به درستی پیکر بندی شده باشد . اصولا PING یکی از بهترین دستورات برای پیدا کردن ایراد در شبکه است .

OPTION های مختلف دستور PING :

۱) PING-T : با استفاده از پارامتر T میتوان تعیین کرد تا دستور PING تا زمان ایجاد وقفه توسط کاربر به PINGکردن ادامه دهد . یعنی کار ارسال بسته تا بی نهایت ادامه یابد . مگر اینکه کاربر آن را متوقف کند .

۲) PING-A : با استفاده از پارامتر A نیز می توان نام هاست آی پی مورد نظر را پیدا کرد . به عبارتی این پارامتر نام هاست متناظر با آی پی را نمایش می دهد .

۳) PING-N : با استفاده از پارامتر N نیز میتوان تعداد دفعات ارسال ECHO REQUEST MESSAGES که به طور پیش فرض ۴ بار میباشد را افزایش یا کاهش داد .

۴) PING – L : با استفاده از پارامتر L نیز میتوان حجم بسته ECHO REQUEST MESSAGES را که به طور پیش فرض ۳۲ بایت می باشد تغییر داد . ماکزیمم مقدار مجاز برای این پارامتر ۶۵۵۲۷ می باشد

۵) PING-I : با استفاد ها از پارامتر I نیز میتوان مدت زمان زنده بودن PACKET سرگردان را تعیین کرد . به عبارت دیگر این پارامتر TTL ، TIME TO LIVE - بسته ECHO REQUEST MESSAGES را تعیین میکند .

۶) PING – V : با استفاده از پارامتر V نیز میتوان مقدار TOS – TYPE OF SERVICE در هدر آی پی ECHO REQUEST MASSAGES رو تعیین کرد . مقدار پیش فرض ۰ می باشد . محدوده مجاز این مقدار نیز بین ۰ و ۲۵۵ می باشد .

۷) PING-W : با استفاده از پارامتر W نیز می توان مدت زمان انتظار برای دریافت پاسخ از هاست برحسب میلی ثانیه تعیین نمود .

۴) دستور TRACERT :

همانطور که از نام این ابزار پیداست ، از TRACERT برای پیدا کردن مسیر بین دو HOST یا به عبارتی دو دستگاه دارای آدرس شبکه که همدیگر را می بینند استفاده می شود . یعنی اینکه بسته ی ارسالی ما برای رسیدن از مبدا به مقصد از چه دستگاه هایی عبور میکند این دستور از طریق پروتکل ICMP این کار را انجام می دهد و آن بدین صورت است که بسته ECHO REPLY ایجاد شده و به کامپیوتر مبدا ارسال می شود .

این دستور علاوه بر اینکه اطلاعات جامعی از هریک از مسیریاب های مسیر تا رسیدن به مقصد به ما می دهد بلکه نام آن مسیریاب ها را در صورتی که در آنها تنظیم شده و در دسترس قرار گرفته باشد نشان خواهد داد .

همچنین زمان رفت و برگشت بسته ICMP ما از مبدا تا مسیریاب بین راه ، برمبنای میلی ثانیه نیز توسط این دستور مشخص خواهد شد . این اطلاعات به ما کمک خواهد کرد تا کشف کنیم در کجای مسیر ارتباطی بین دو نقطه از شبکه مشکل وجود دارد.

درصورت مشکل در مسیر ارتباطی به مقصد ، TRACE ROUTE های ما موفقیت آمیز نخواهد بود .

مانند مثال زیر :

C:\>tracert comptia.org

Tracing route to comptia.org [216.119.103.72]

over a maximum of 30 hops5

1 27 ms 28 ms 14 ms 24.67.179.1

2 55 ms 13 ms 14 ms rd1ht-ge3-0.ok.shawcable.net [24.67.224.7]

3 27 ms 27 ms 28 ms rc1wh-atm0-2-1.shawcable.net [204.209.214.19]

4 28 ms 41 ms 27 ms rc1wt-pos2-0.wa.shawcable.net [66.163.76.65]

5 28 ms 41 ms 27 ms rc2wt-pos1-0.wa.shawcable.net [66.163.68.2]

6 41 ms 55 ms 41 ms c1-pos6-3.sttlwa1.home.net [24.7.70.37]

7 54 ms 42 ms 27 ms home-gw.st6wa.ip.att.net [192.205.32.249]

8 * * * Request timed out

در این مثال ، بسته ارسالی ICMP ما تنها موفق شده تا ۷ مرحله پیش رود و در مرحله ۸ ام به مشکل برخورد کرده است که دلیل آن می تواند این باشد که دستگاهی که در مرحله ۸ ام قرار داد قطع است و یا اینکه دستگاه موجود در مرحله ۷ ام کار میکند اما امکان مشخص کردن هاست بعدی را ندارد .

۵) دستور NET STAT :

NET STAT ، مخفف NETWORK STATISTICS ، یک ابزار خط فرمان است که اتصالات شبکه را ، جداول هدایت کردن بسته ها و تعدادی از آمار رابطه های شبکه ای را نشان می دهد . همچنین این ابزار برای پیدا کردن مشکلات در شبکه و برآورد حجم اطلاعات رد و بدل شده به عنوان یک اندازه گیر عملکرد استفاده می شود .

پارامتر های ورودی :

پارامتر هایی که در ورودی همراه دستور وارد می شوند باید با – شروع شوند (در ویندوز امکان استفاده از / نیز وجود دارد)

دستور NETSTAT بدون پارامتر : نمایش CONNECTION های فعال

NETSTAT-A : نمایش تمامی اتصالات TCPو UDP فعال در کامپیوتر

NETSTAT-B : نمایش برنامه ی درگیر با اتصالات شبکه ای نمایش داده شده در لیست خروجی

NETSTAT-E : نمایش آمار مربوط به اترنت ، از قبیل تعداد بایت ها و بسته های دریافتی و ارسالی

NETSTAT-F : نمایش FQDN برای آدرس های خارجی (فقط در ویندوز ویستا و سیستم عامل های جدیدتر)

NETSTAT-N : نمایش ارتباط های TCP فعال ، هرچند که IP ها و پورت هارا به صورت عددی نمایش می دهد و تلاشی برای تشخیص نام آنها نمیکند .

NETSTAT-M : نمایش آمار مربوط به استریم ها

NETSTAT-O : نمایش اتصال های TCP فعال به همراه PID مربوط به آن اتصال

NETSTAT-P : در ویندوز پروتکل مربوط به اتصال را نشان می دهد .

NETSTAT-R : جدول هدایت IP ها را نشان می دهد .

NETSTAT-S : نمایش آمار به تفکیک پروتکل

NETSTAT-/? : نمایش راهنمایی برای دستورات موجود (فقط در ویندوز)

۶) دستور NET :

این دستور بیشتر برای کار با OBJECT های شبکه ای مورد استفاده قرار می گیرد . با این دستور باید کلمه ای دیگر مانند USER و COMPUTER تا سیستم متوجه بشود که می خواهید با چه نوع OBJECT ی کار کنید.

در زیر چند نمونه از این دستور را مشاده می کنید .

NET ACCOUNTS : با این دستور وضعیت تنظیم پسوورد ها (مثل طول عمر پسوورد ها) نشان داده

می شود .

NET COMPUTER : کامپیوتر ها را به پایگاه داده ای DOMAIN مورد نظر اضافه و یا کم میکند .

NET CONTINUE : سرویسی که توسط دستور NET PAUSE معلق شده است را دوباره راه اندازی میکند.

NET FILE : نام تمامی فایل های باز و اشتراک گذاشته شده بر روی سرور را نمایش می دهد .

NET GROUP : لیست گروه های محلی تعریف شده را بیان می کند و نیز میتوان فهمید در هرکدام از این گروه ها چه اکانت هایی وجود دارد و نیز میشود به یه گروه خاص اکانتی اضافه کرد .

اگر بخواهیم ببینیم چه گروه های محلی تعریف شده است می نویسیم : NET LOCALGROUP

NET HELPMSG : وقتی که یک دستور NET به صورتی اجرا می شود که خطایی پیش بیاید ، ویندوز یه شماره خطای ۴ رقمی به ما می دهد که برای جزئیات بیشتر در مورد این خطا باید از دستور

NET HELPMSG استفاده کنیم .

NET PAUSE : سرویس های در حال اجرا را متوقف می کند .

NET LOCALGROUP : گروه های محلی را نمایش ، اصلاح یا اضافه میکند .

NET SHARE : این دستور به ما کمک می کند SHARE ها را به صورت محلی مدیریت کنیم .

NET STATISTICS : آمار مربوط به سرور ها را نشان می دهد .

NET START : سرویس های شبکه را آغاز یا لیست می کند .

دستور دیگر NS LOOKUP است که یکی دیگر از راه های بدست آوردن DNS ها می باشد .

برای هک کردن هم استفاده میشه این دستور .

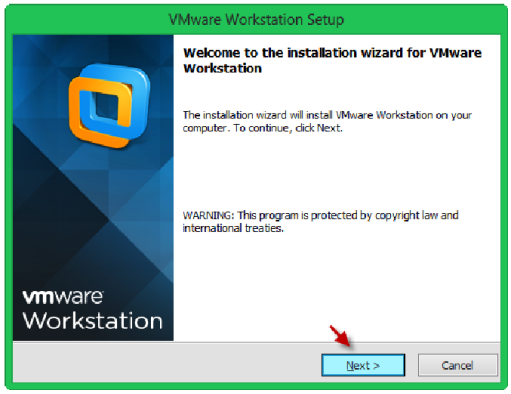
راهنمای نصب و راه اندازی

Wmware Workstation

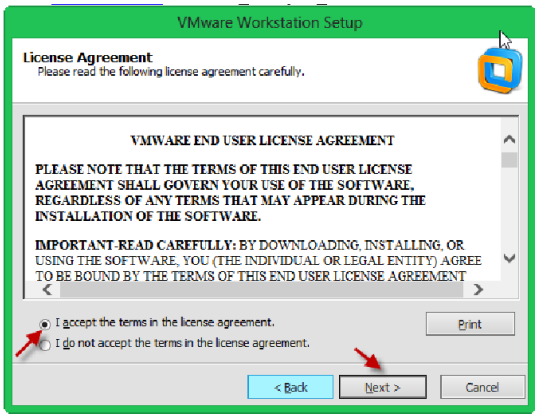
بعد از دریافت نرم افزار روی setup کلیک کنید وstart کنید:

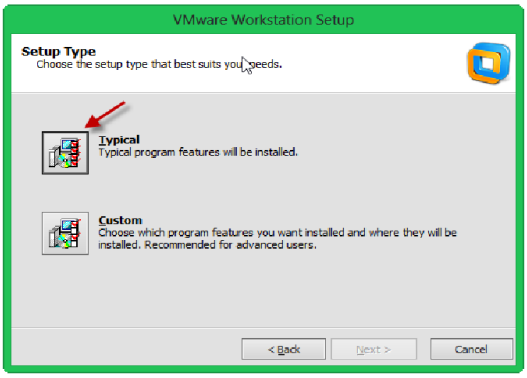
نرم افزار در حال خارج شدن از حالت فشرده و اجرای حالت اصلی.

در این صفحه بر روی next کلیک کنید.



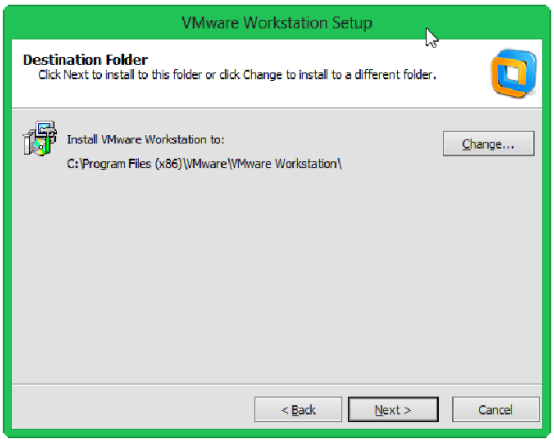
در این قسمت توافقنامه این نرم افزار را خوانده و اگر قبول دارید روی گزینه I Accept کلیک کنید و بعد روی Next کلیک کنید



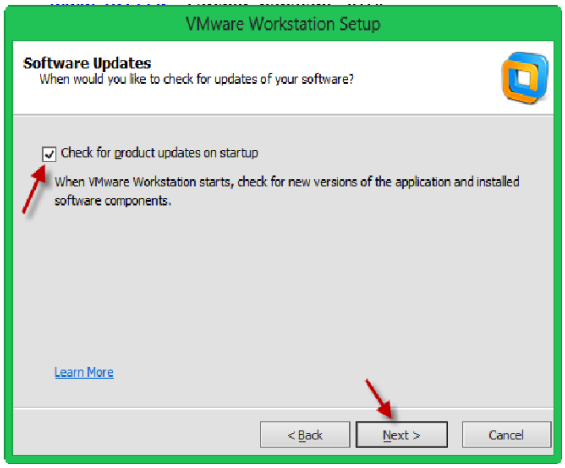


در این قسمت روی Typical کلیک کنید.

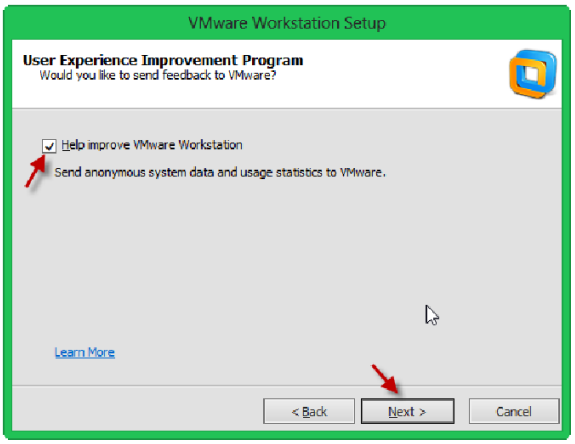
در این قسمت با کلیک بر روی ...Change می توانید مسیر نصب برنامه را مشخص کنیدو بعد از این کار بر روی Next کلیک کنید.



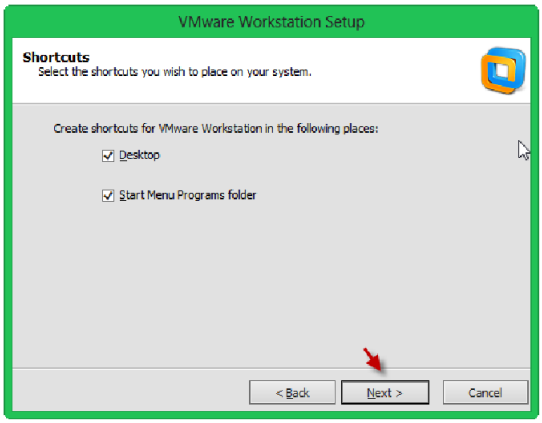
در این قسمت اگر نرم افزاری که در حال نصب آن هستید یک نرم افزار با سریال نامبر خریداری شده باشد تیک گزینه Check for Product Updates on startup را بزنید تا ماشین مجازی در حال اجرا به دنبال نسخه جدید خود بگردد اگر هم این نسخه کرک شده است این کار لازم نیست. بر روی Next کلیک کنید.



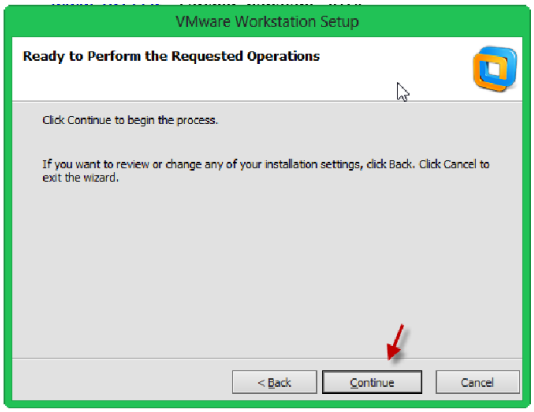
در این قسمت هم مانند قسمت قبلی اگر نرم افزار اصلی است و کرک شده نمی باشد بر روی گزینه مورد نظر کلیک کنید تا مشکلات احتمالی این نرم افزار به سایت اصلی آن فرستاده شود.بر روی Next کلیک کنید.



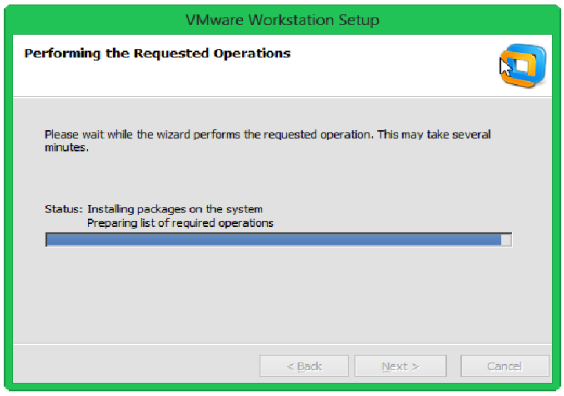
در این صفحه با انتخاب گزینه های مورد نظر shortcut این نرم افزار در محل های مشخص شده برای اجرا قرار می گیرد . بر روی Next کلیک کنید.



در این قسمت برای نصب بر روی Continue کلیک کنید.



نرم افزار در حال نصب می باشد.....

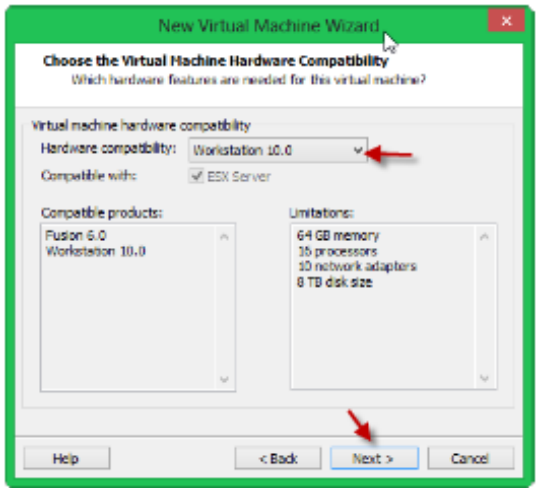


نصب نرم افزار به پایان رسیده و بر روی Finish کلیک کنید

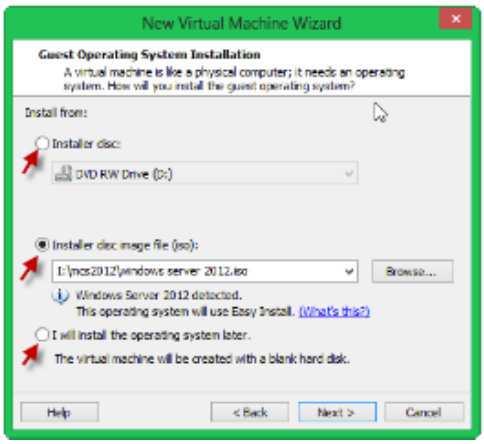
در این بخش می توانیم یک ماشین مجازی با امکانات سخت افزاری و نرم افزاری متفاوت ایجاد کنیم . برای انجام این کار بر روی گزینه مورد نظر کلیک کنید.

در این قسمت دو گزینه موجود است که یکی بصورت تنظیمات سریع و آسان و یکی دیگر بصورت تنظیمات پیشرفته وجود دارد که می توانیم نوع هارد دیسک ، نحوه ذخیره سازی و ..... را مشخص کنیم در این آموزش گزینه دوم را انتخاب می کنیم تا گزینه اول را هم گفته باشیم،بعد از انتخاب گزینه مورد نظر بر روی Next کلیک کنید.

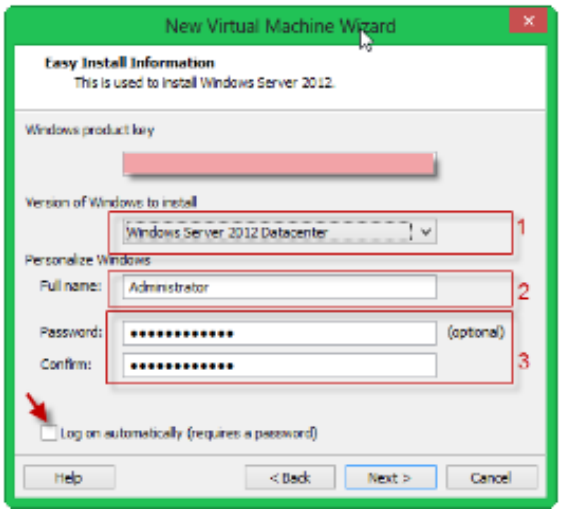
در این قسمت گزینه اول را انتخاب کنید تا تمام نرم افزارهای جدید را بتوان روی این ماشین مجازی اجرا کرد.مثلا ویندوز سرور ۲۰۱۲ را نمی توانید روی VMware 8 اجرا کنید . بعد از انتخاب گزینه اول بر روی Next کلیک کنید.



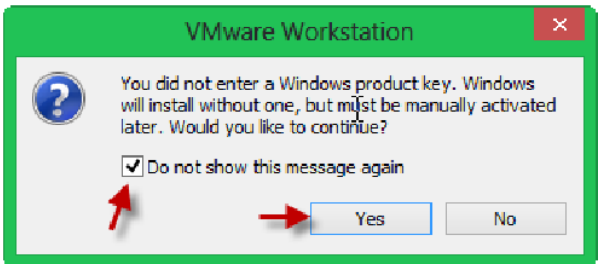
در این قسمت شما باید ، برای ماشین مجازی مشخص کنید که چه چیزی را باید اجرا کند اگر قسمت اول را انتخاب کنید سیستم عامل از طریق DVD/CD خوانده می شود ، در قسمت دوم می توانید سیستم عامل خود را از طریق فایل ISO معرفی کنید و در قسمت آخر می توانید معرفی سیستم عامل را به بعد موکول کنید. در این قسمت ویندوز سرور ۲۰۱۲ را می خواهیم اجرا کنیم که در قسمت دوم وارد کردیم.



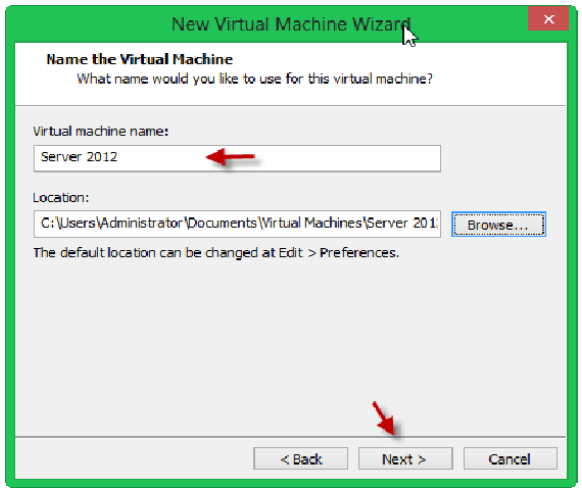
در این قسمت که برای راحتی کار شما طراحی شده است می توانید در قسمت Product Key رمز عبور سیستم عامل خود را وارد کنید که شاید ویندوز شما کرک شده باشد و لازم به وارد کردن رمز نداشته باشد ، در قسمت های بعدی که با شماره مشخص شده است در قسمت اول ورژن سیستم عامل خود را مشخص کنید . در قسمت های دو و سه نام کاربری و رمز عبور مربوط به سیستم عامل مورد نظر را مشخص کنید تا از شما در زمان نصب سیستم عامل سوال نشود، در قسمت آخر اگر تیک گزینه Log On automatically را بزنید به صورت خود کار وارد ویندوز می شود البته توسط نام کاربری و رمز عبوری که در قسمت دو و سه مشخص می کنید. بعد از وارد کردن اطلاعات بر روی Next کلیک کنید.



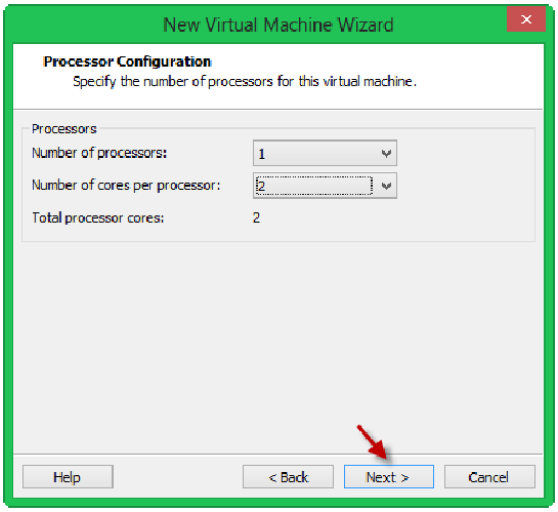
این پنجره زمانی ظاهر می شود که شماره سریال را وارد نکرده باشید و می گوید که باید به صورت دستی ویندوز را فعال کنید



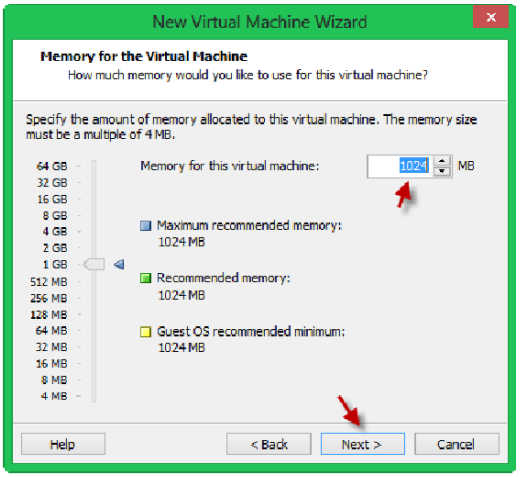
در قسمت اول نام سیستم عامل خود را وارد کنید و در قسمت Location آدرس ذخیره شده این ماشین را مشخص کنید،در پایان روی Next کلیک کنید.



در قسمت Number of processors تعداد CPU سیستم اصلی خود را مشخص کنید و در قسمت Number of cores per processor تعداد هسته CPU خود را مشخص کنید، اگر بیشتر از حد انتخاب کنید به شما اخطار داده می شود .



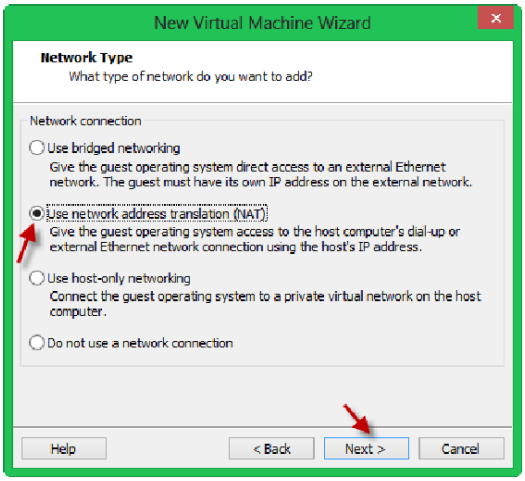
در این قسمت به اندازه نیاز خود و به اندازه رم سیستم خود می توانید برای این ماشین مجازی حافظه ایجاد کنید. اگر توجه کنید سه مربع زرد ، سبز، آبی وجود دارد که می توانید با انتخاب هر کدام ازانها مقدار حافظه مورد نیاز سیستم را مشخص کنید، البته اگر بر روی رنگ سبز کلیک کنید مقدار حافظه متعادل به نسبت سیستم شما برای این ماشین مجازی در نظر می گیرد



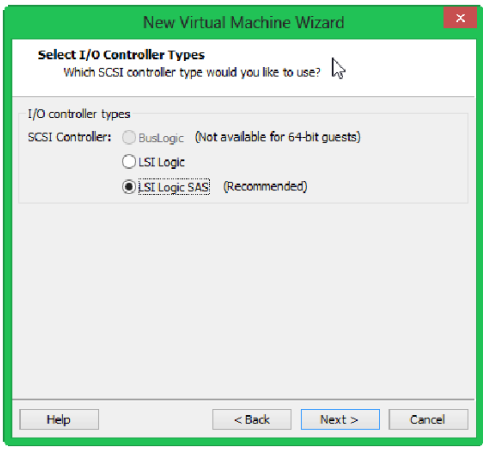
.

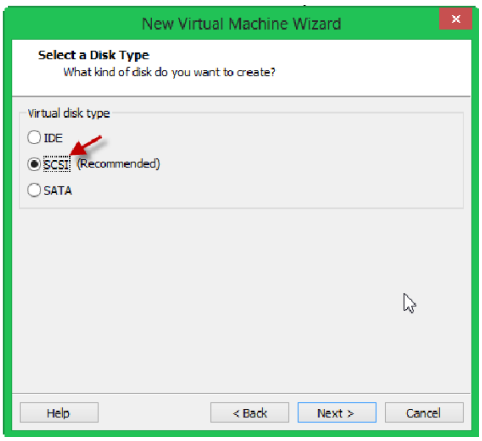
در این قسمت گزینه های مختلف برای ارتباط کارت شبکه با شبکه های مختلف وجود دارد که اگر قسمت اول را انتخاب کنید می توانید با کارت شبکه اصلی سیستم خود ارتباط داشته باشید،گزینه دوم هم به صورت کارت شبکه مجازی به شبکه متصل می شود، گزینه سوم هم برای ارتباط داخلی شبکه خود سیستم عامل می باشد ، و با انتخاب گزینه آخر سیستم عامل به شبکه متصل نمی شود، که در اینجا گزینه دوم انتخاب می شود و بر روی Next کلیک کنید.

در این قسمت نوع I/O controller را مشخص کنید که زیاد هم مهم نمی باشد.بر روی Next کلیک کنید.

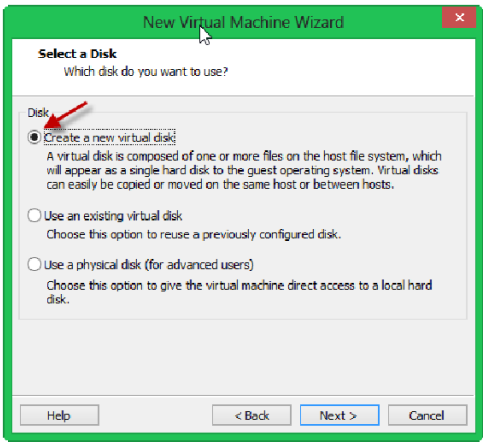


در این قسمت نوع ارتباط هارد دیسک مجازی را انتخاب کنید ، که سعی کنید روی پیش فرض قرار داشته باشد و تغییر ندهید، بر روی Next کلیک کنید.

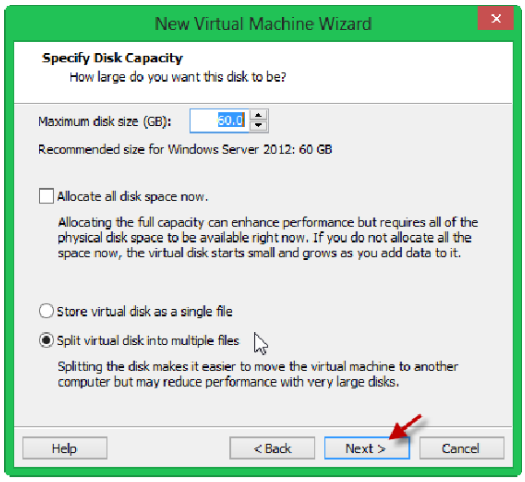




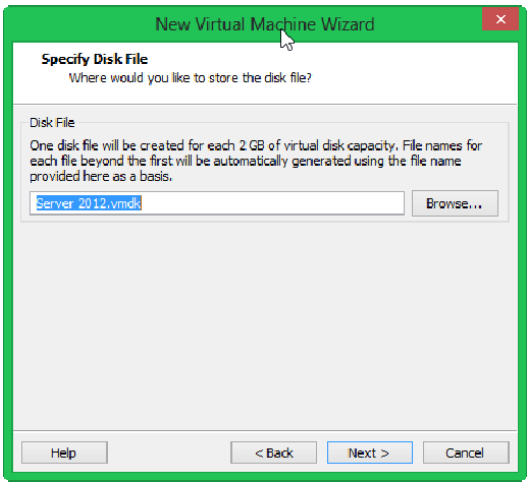
در این قسمت سه گزینه وجود دارد که با انتخاب گزینه اول می توانید هارد دیسک مجازی جدید ایجاد کنید، در قسمت دوم می توانید هارد دیسکی را که قبلا ایجاد کرده اید به این ماشین معرفی کنید مثلا شاید شما یک ویندوز نصب کرده باشید ، از طریق این روش می توانید هارد دیسک آن ویندوز را به این ماشین معرفی کنید، گزینه اخر هم استفاده مستقیم از هارد دیسک اصلی سیستم می باشد ،گزینه اول را انتخاب و بر روی Next کلیک کنید.



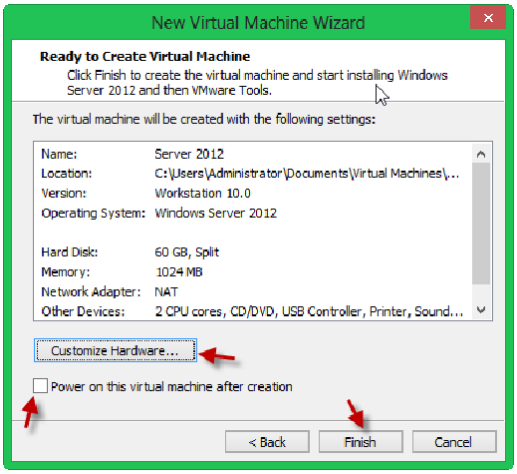
در قسمت Maximum می توانید مقدار اختصاصی داده شده به هارد دیسک مجازی را مشخص کنید،اگر تیک گزینه Allocate all disk space now را بزنید یعنی اینکه کل این فضای ۶۰ گیگا بایت به این ماشین مجازی اختصاص داده می شود و اشغال می شود که این کار را انجام ندهید دو گزینه اخر هم برای مشخص کردن ذخیره اطلاعات در یک فایل تکی یا چند فایل می باشد که می توانید یکی از آنها را انتخاب کنید ، بر روی Next کلیک کنید.



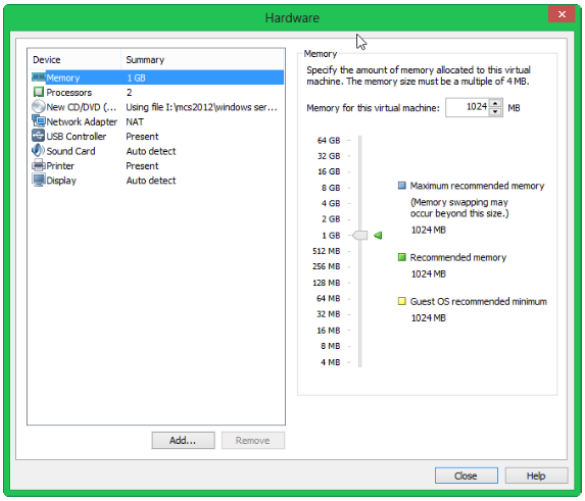
در این قسمت می توانید هارد دیسک مجازی خود را در محل مورد درخواستی خود ذخیره کنید و از این فایل بعد ها استفاده کنید.بر روی Next کلیک کنید.



در این قسمت کل اطلاعات وارد شده را به صورت خلاصه به شما نمایش می دهد . اگر تیک گزینه Power on this virtual machine را بردارید بعد از اینکه بر روی Finish کلیک کنید، سیستم خود به خود روشن نمی شود . اگر بر روی Customize Hardware کلیک کنید می توانید سخت افزار این ماشین مجازی را مانند شکل مشاهده کنید.



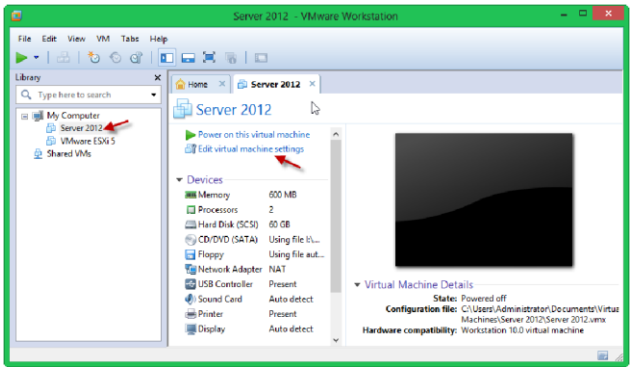
همانطور که مشاهده می کنید ، کل سخت افزار این سیستم را می توانید مشاهده کنید و یا آن ها را می توانید تغییر دهید. بر روی Close کلیک و بر روی Finish کلیک کنید تا کار نصب به پایان برسد.



ارتباط ماشین مجازی با شبکه :

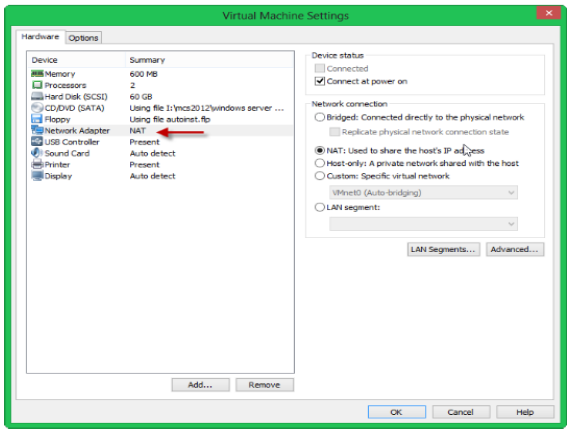
زمانی که یک ماشین مجازی ایجاد می کنیم ، این ماشین می تواند با روش های مختلف به شبکه های اصلی و مجازی متصل شود. این روش ها را بررسی می کنیم.

برای نمایش شبکه های ماشین مجازی بر روی ماشین مجازی مورد نظر مانند شکل زیر کلیک راست کرده و بر روی Edit virtual machine settings کلیک کنید.



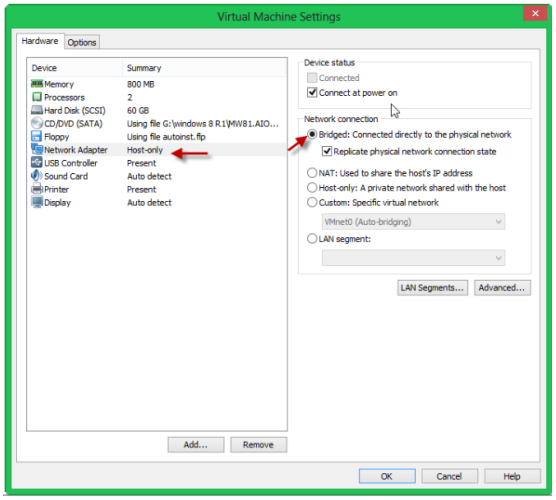
در صفحه باز شده بر روی Network Adapter کلیک کنید تا لیست ارتباط های مختلف شبکه نمایان شود ، اگر قسمت Bridged را انتخاب کنید ، کارت شبکه ماشین مجازی شما مستقیما به کارت شبکه ویندوز اصلی شما متصل می شود ، اگر هم تیک گزینه مورد نظر را بزنید کارت شبکه کاملا همگام با کارت شبکه اصلی کار می کند.وهر تغییری در کارت شبکه اصلی بر روی کارت شبکه مجازی تاثیر می گذارد.

اگر کارت شبکه اصلی شما متصل به اینترنت باشد با این روش می توانید ماشین مجازی را به اینترنت متصل کنید ، برای همین کاریک ماشین مجازی که قبلا ایجاد کرده ایم را بر روی Bridged قرار می دهیم و به اینترنت متصل می کنیم .

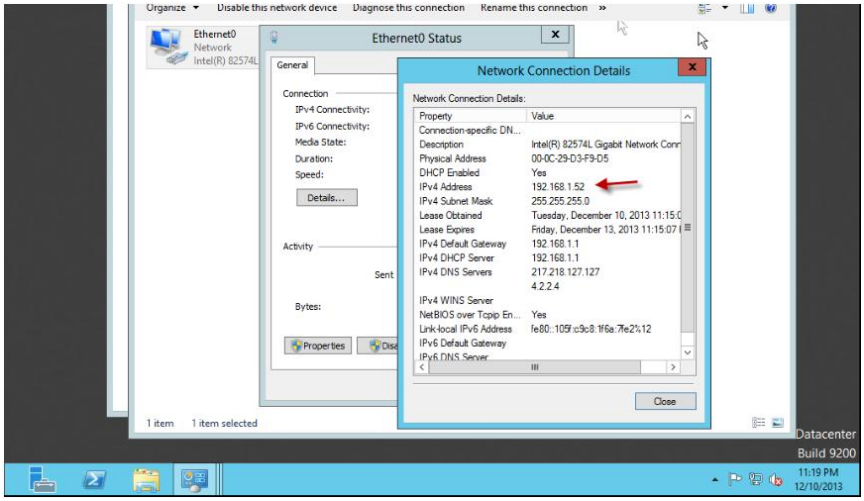


کارت شبکه سیستم اصلی که به اینترنت متصل است از یک مودم ADSL به صورت DHCP آدرس IP گرفته است. این آدرس IP به شماره ۱۹۲,۱۶۸,۱,۵۰ می باشد.

همانطور که مشاهده می کنید از سمت چپ بر روی Network Adapter کلیک می کنیم و بعد از آن از سمت راست گزینه ...Bridged را انتخاب می کنیم و بعد OK می کنیم .اگر وارد ویندوز مجازی خود شوید متوجه اتصال شبکه آن با شبکه اصلی خود می شوید.



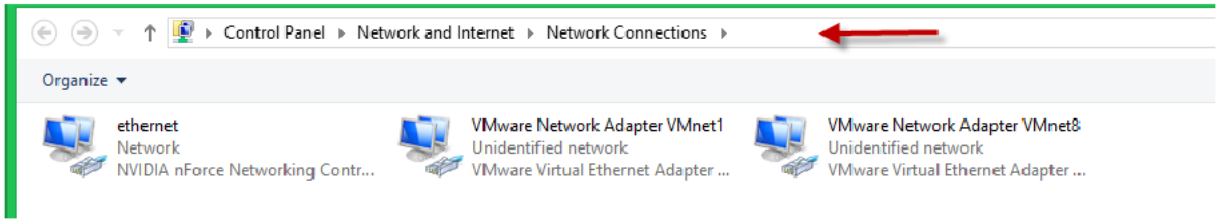
همانطور که در شکل زیر مشاهده می کنید ویندوز مجازی با استفاده از ویژگی Bridged به شبکه اصلی سیستم متصل شده است و آدرس 192.168.1.52 را از طریق مودم ADSL متصل به سیستم اصلی دریافت کرده است و همینطور قابلیت اتصال به اینتر نت را هم بدست آورده است.



اگر سرویس DHCP فعال نباشد باید به شبکه اصلی خود به صورت دستی آدرس دهید و به شبکه مجازی خود هم باید در رنج شبکه اصلی خود آدرس دهید تا ارتباط این دو ویندوز با هم بر قرار شود.

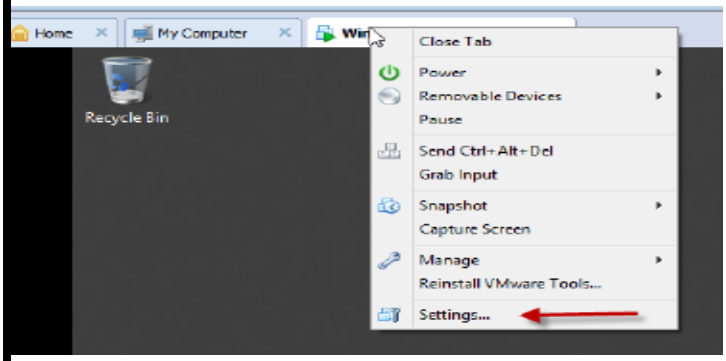
ارتباط از طریق NAT :

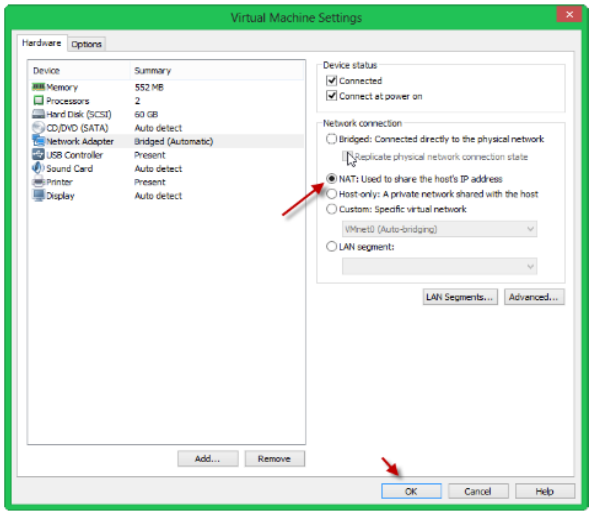
در این ارتباط ، ماشین مجازی از طریق کارت شبکه مجازی که مختص نرم افزار VMware می باشد به شبکه متصل می شود ، همانطور که قبلا گفتیم ماشین مجازی بعد از نصب، دو کارت شبکه مجازی را به صورت پیش فرض بر روی سیستم شما ایجاد می کند، البته می توانید این کارت شبکه ها را اضافه یا حذف کنید که در ادامه به آن می پردازیم. اگر در ویندوز اصلی خود وارد مسیر زیر شوید متوجه ایجاد دو کارت شبکه خواهید شد و ویندوز مجازی شما زمانی که روی NAT باشد از این کارت های شبکه مجازی استفاده می کند.



برای قرار دادن شبکه روی NAT از طریق زیر اقدام می کنیم :

برای وارد شدن به قسمت Settings هر ماشین مجازی راه های مختلفی وجود دارد که یکی از این راهها کلیک راست کردن روی ماشین مجازی و انتخاب Settings می باشد.

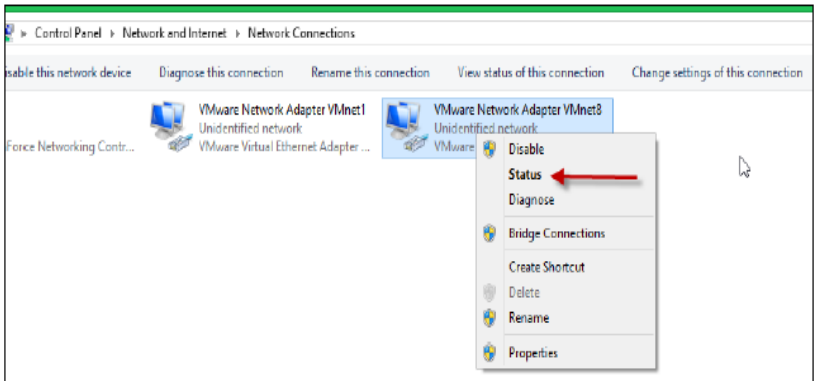




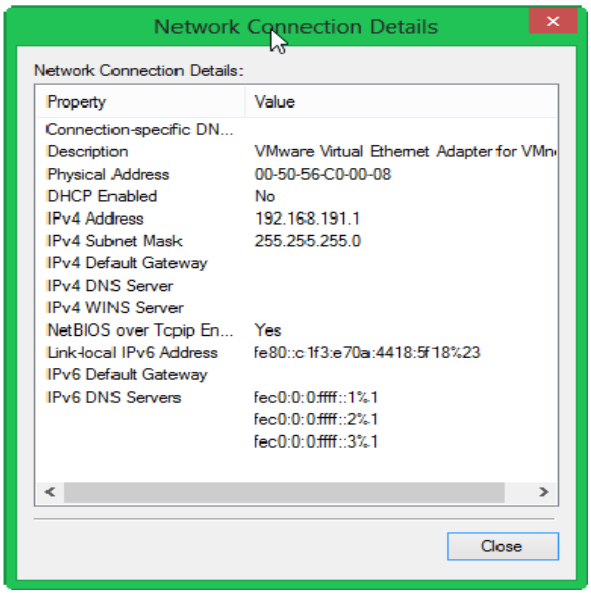
بعد از ظاهر شدن صفحه مورد نظر گزینه NAT را انتخاب و بر روی OK کلیک کنید.

بعد از انجام این کار کارت شبکه ویندوز مجازی با کارت شبکه مجازی داخل ویندوز اصلی ارتباط برقرار می کند.

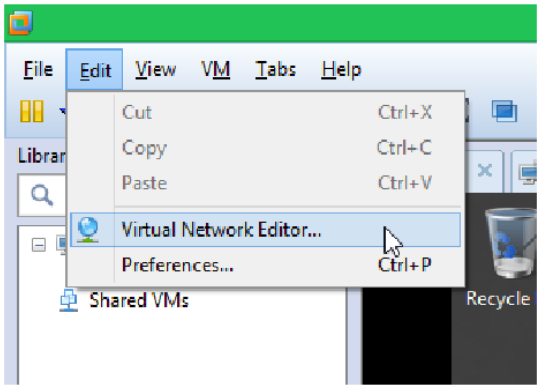
وارد Network Connections در ویندوز اصلی شوید و روی آیکون کارت شبکه مجازی VMnet8 کلیک راست کنید و گزینه Status را انتخاب کنید.



بعد از ظاهر شدن صفحه مورد نظر بر روی Details کلیک کنید تا مشخصات ظاهر شود همانطور که مشاهده می کنید رنج IP این کارت شبکه مجازی ۱۹۲,۱۶۸,۱۹۱,۱ می باشد و اگر وارد ویندوز مجازی شوید و به همین صورت بالا این صفحه را باز کنید متوجه می شوید که این دو در یک رنج قرار داد ، به شکل توجه نمایید :



همانطور که مشاهده می کنید کارت شبکه این ویندوز مجازی در رنج کارت شبکه مجازی ویندوز اصلی با نام VMnet8 قرار دارد .شاید برای شما سوال پیش بیاید که این کارت شبکه های مجازی چگونه ایجاد شده اند.برای دریافت این موضوع باید به منوی Edit برویم و گزینه Virtual Network Editor را انتخاب کنیم ، مانند شکل روبرو .

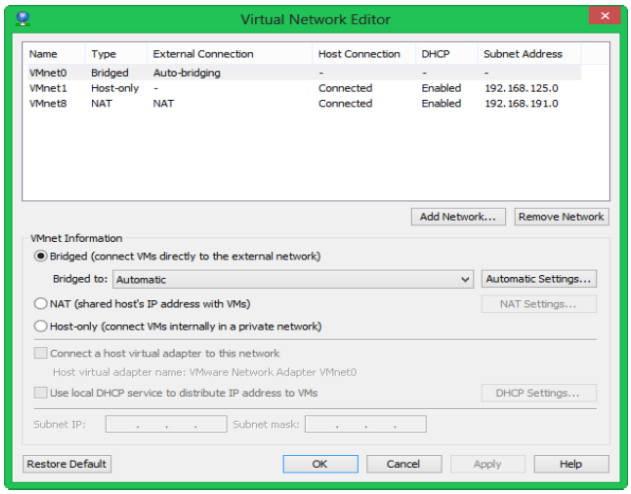


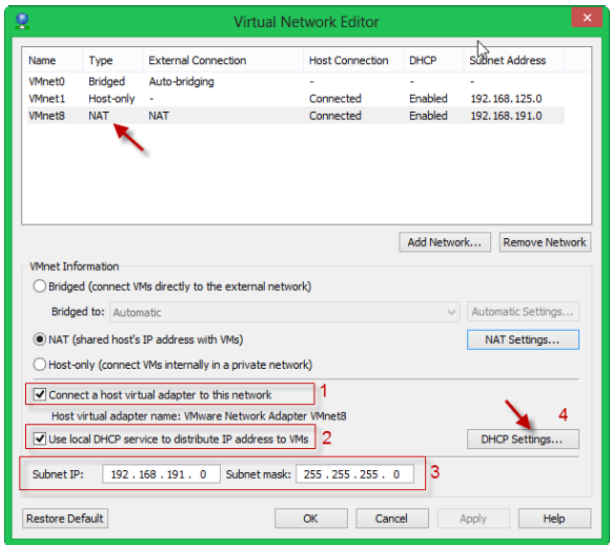
همانطور که مشاهده می کنید در این صفحه ۳ کارت شبکه مجازی ایجاد شده که هر کدام کارهای خاصی انجام می دهند.

کارت شبکه با نام VMnet0 که در لیست مشاهده می کنید.اگر روی آن کلیک کنید متوجه می شوید که این کارت شبکه از نوع Bridged بوده و با کارت شبکه اصلی در ارتباط است.در قسمت VMnet Information می توانید تنظیمات مختلف را انجام دهید.

شاید بر روی سیستم خود از دو کارت شبکه استفاده می کنید می توانید با کلیک بر روی لیست کشویی Bridged to کارت شبکه مورد نظر را انتخاب کنید یا اینکه Automatic قرار دهید.

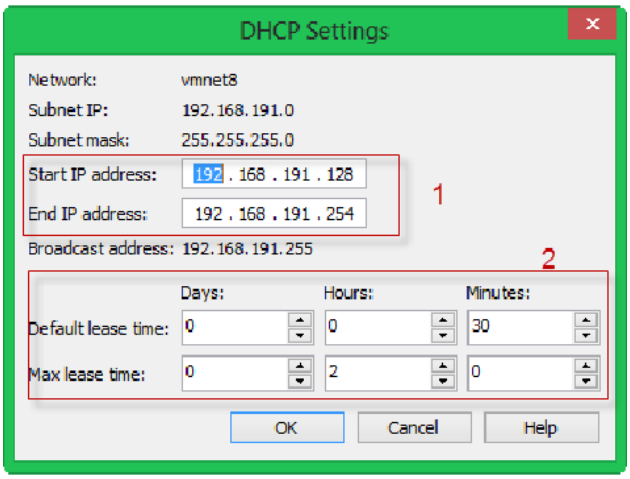
گزینه بعدی NAT می باشد که توضیح دادیم ، بعد از انتخاب NAT گزینه های آن فعال می شوند ، اگر تیک قسمت ۱ را بزنید این شبکه با کارت شبکه مجازی ایجاد شده در داخل ماشین مجازی شما ارتباط برقرار می کند ، اگر تیک گزینه دوم را بزنید این کارت از سرویس DHCP استفاده می کند که می توانید در قسمت ۳ شماره آدرس شبکه خود را وارد کنید و در قسمت DHCP settings می توانید سرویس DHCP را تنظیم کنید مانند زیر :

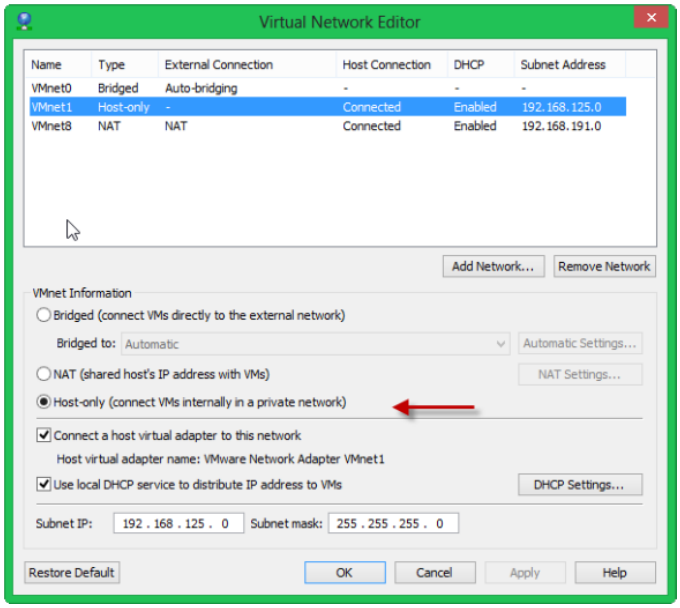




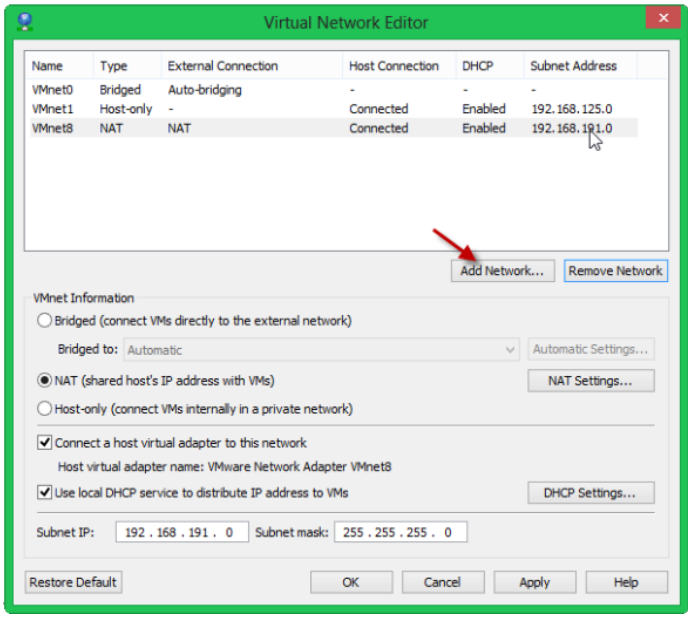
در قسمت شماره یک شروع آدرس و پایان آدرس برای اختصاص دادن به کلاینت ها را نوشته ،یعنی اگر یک کلاینت بخواهد از این شبکه IP بگیرد از ۱۹۲,۱۶۸,۱۹۱,۱۲۸ به بعد IP می گیرد و در قسمت ۲ زمان پیش فرض Lease و حداکثر زمان Lease مشخص شده است اگر در این زمان مشخص شده کلاینت حضور خود را اعلام نکند این IP از وی پس گرفته و به کلاینت دیگر داده می شود .

اگر گزینه VMnet1 را انتخاب کنید یعنی ارتباط فقط بین دو شبکه مجازی صورت می گیرد و قابلیت اتصال به اینترنت ندارد ، اگر به شکل توجه کنید گزینه HOST-ONLY را انتخاب کردیم که فقط ارتباط بین دو شبکه مجازی است یعنی ارتباط کارت شبکه مجازی VMnet1 با کارت شبکه ماشین مجازی .اگر قسمت NAT را انتخاب کنید بخاطر Share کردن Host به اینترنت متصل می شود . این شبکه هم مانند NAT از سرویس DHCP استفاده می کند.

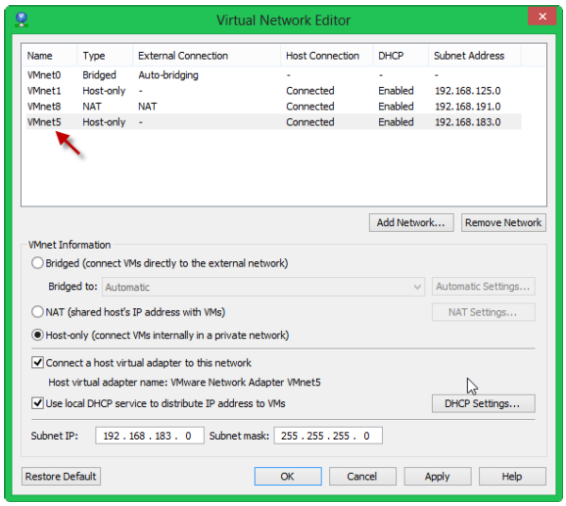




برای اضافه کردن کارت شبکه مجازی بر روی سیستم اصلی خود بر روی Add Networkکلیک کنید و از بین ۱۷ کارت شبکه یکی را انتخاب کنید ، در کل در این نرم افزار ۲۰ کارت شبکه می توانیم ایجاد کنیم که به صورت پیش فرض ۳ تا از آن ها ایجاد شده اند.بعد از انتخاب کارت شبکه می توانید آن را مانند قبل که توضیح داده شد تنظیم کنید.

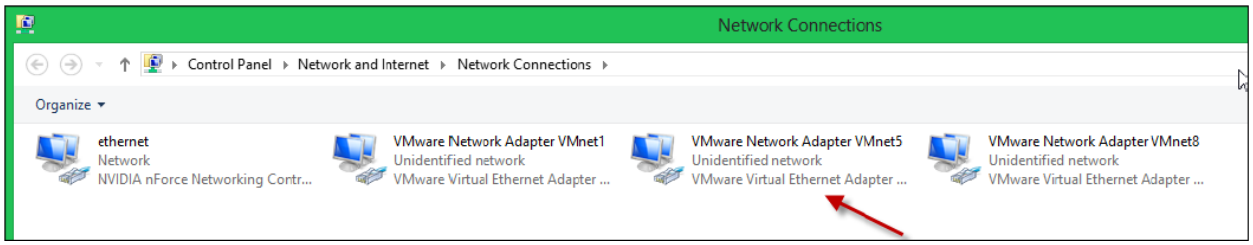


همانطور که مشاهده می کنید کارت شبکه VMnet5 را به لیست اضافه کردیم ، یک نکته در این قسمت وجود دارد و آن این است که در یک زمان دو کارت شبکه نمی توانند در حالت NAT و Bridged قرار بگیرند و فقط یک کارت شبکه می تواند در این حالت قرار بگیرد.بعد از ok کردن و ایجاد شبکه جدید اگر به Network Connections سیستم خود نگاهی بیندازید متوجه می شوید که این کارت شبکه مجازی به لیست اضافه شده است مانند زیر :



به صورت کلی اگر کارت شبکه ماشین مجازی خود را بر روی Bridged قرار دهید با کارت شبکه اصلی و فیزیکی سیستم شما ارتباط بر قرار می کند ، اگر بر روی NAT قرار دهید با کارت شبکه مجازی که به صورت پیش فرض Vmnet8 می باشد ارتباط برقرار می کند و به علت Share بودن Host از اینترنت سیستم شما استفاده می کند. و اگر هم بر روی Host-Only قرار دهید

این شبکه فقط با کارت شبکه مجازی ارتباط برقرار می کند و هیچ ارتباطی با دنیای بیرون ندارد.



نصب وتجهیزات DHCP

حالا شما تا حدودی با نحوه کار DHCP آشنا شدید و نوبت آشنایی با نحوه نصب و پیکر بندی DHCP رسیده است که یک پروسه بسیار ساده ای دارد. از روی پنجره Server Manager که در زمان روشن شدن سیستم نمایش داده می شود Add Role را انتخاب کرده و DHCP Server role را انتخاب کنید. از شما یک سری اطلاعات در مورد Domain ی که کلاینت ها استفاده می کنند، در صورت موجود بودن و یا آدرس DNS Server و کامپیوتری که این Roll را دارد می پرسد و بعد از آن شما می توانید یک Scope ایجاد کنید که در زیر به صورت مفصل بحث خواهد شد و همچنان می توانید مشخص کنید که آیا از DHCPv6 استفاده شود یا خیر و یک سری تنظیمات دیگر.

توجه: اگر در شبکه خود قصد استفاده از Active Directory، DNS و DHCP را دارید بهتر است این سه Roll را با Active Directory همزمان نصب کنید. (این روش نصب به صورت کامل در بخش مراحل نصب اکتیو دایرکتوری در سرور ۲۰۰۳ به صورت کامل بیان شده است.)

ساخت Scope جدید در DHCP Server

با ساخت یک Scope جدید رنج آدرس مورد نظر برای شبکه را انتخاب می کنیم. این رنج Scope نامیده می شود.

پنجره ی ایجاد Scope جدید هم در زمان نصب و هم از طریق کنسول مدیریت DHCP در دسترس می باشد. برای ایجاد Scope جدید می بایست مراحل ذیل را طی کنید:

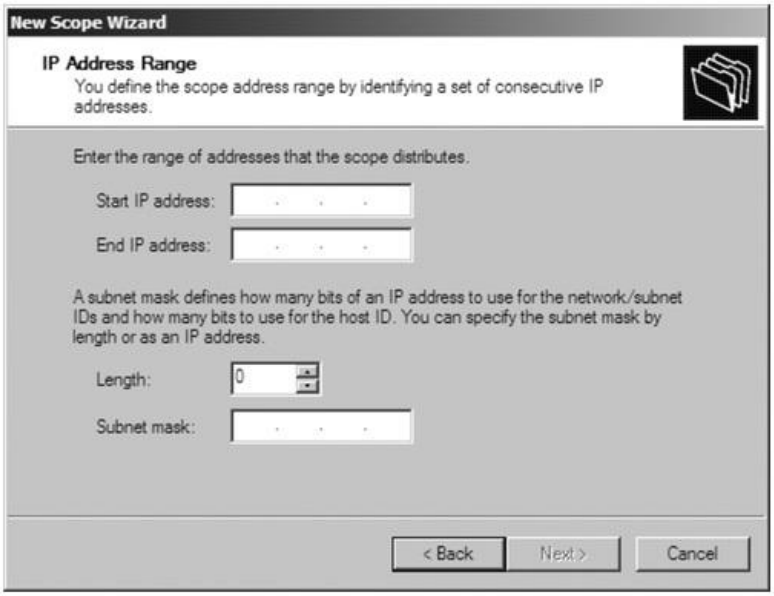
۱. کنسول مدیریت DHCP را از منوی استار سپس Administrator Tools اجرا کنید.

۲. بر روی سرور DHCP از منوی سمت چپ راست کلیک کنید و New Scope <pan> را انتخاب کنید.

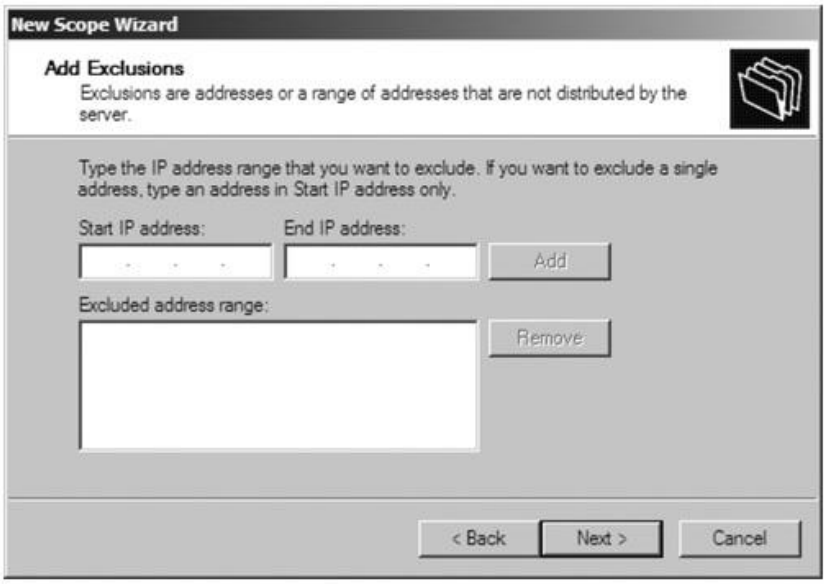
۳. چنجره ایجاد Scope جدید نمایان می شود. روی دکمه Next کلیک کنید.

۴. در صفحه بعد یک نام برای DHCP خود انتخاب کنید و روی Next کلیک کنید.

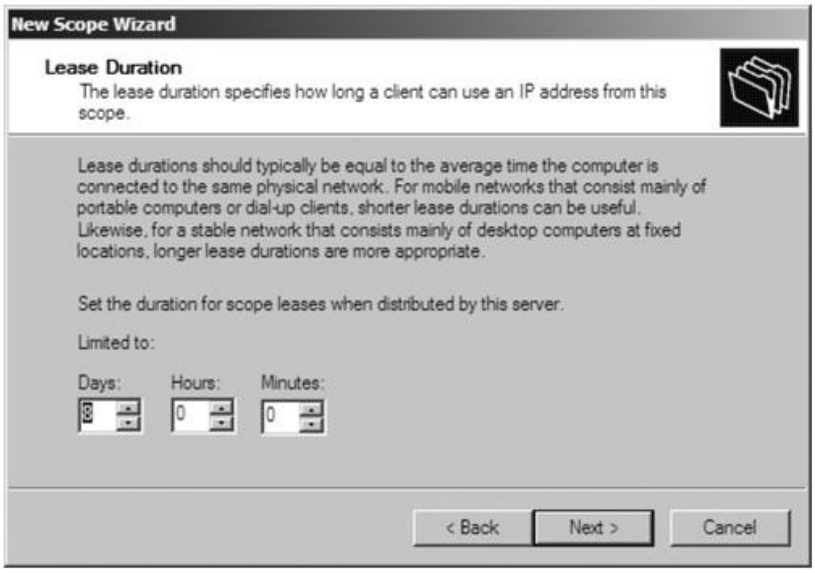
۵. صفحه تعین محدوده آدرس دهی نمایان می شود. اکنون بایستی اولین IP از محدوده ی رنجی که برای کلاینت ها در نظر گرفته اید را در فیلد Star IP address وارد کرده و آخرین IP را در End IP address وارد کنید. سپس Subnet Mask را وارد کنید . و روی Next کلیک کنید.



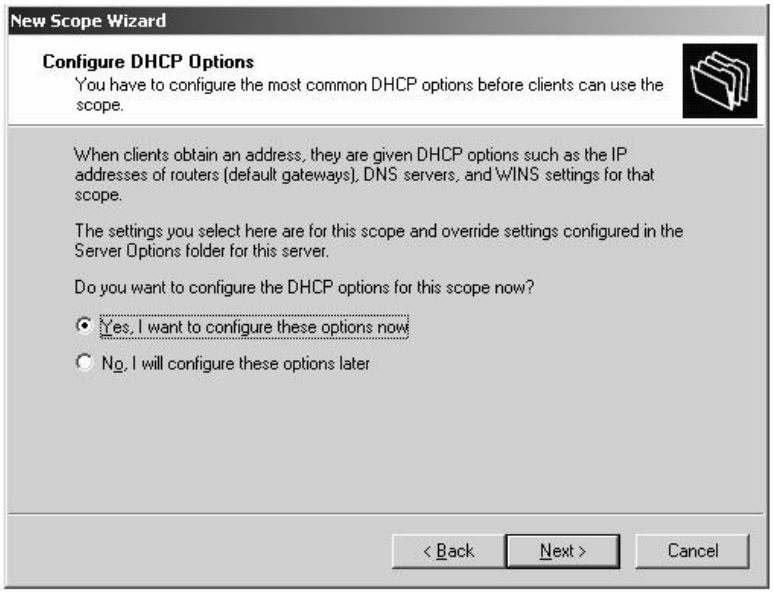
۶. شما می توانید از محدوده ی رنج تعین شده بعضی از IP ها را استثناء قرار دهید به طوری که دیگر به کلاینتی اختصاص داده نشود. به عنوان مثال رنج انتخابی شما بین ۱۰,۱۰,۱۰,۱ تا ۱۰,۱۰,۱۰,۱۰۰ است در این صفحه می توانید به عنوان مثال رنج ۱۰,۱۰,۱۰,۴۰ تا ۱۰,۱۰,۱۰,۴۵ را استثناء قرار دهید.



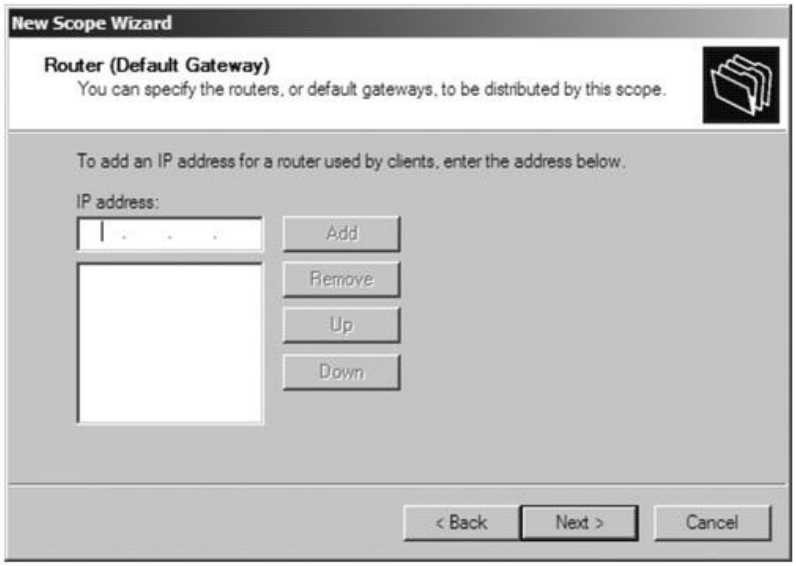
۷. در صفحه Lease Duration می توانید مدت زمان اجاره نامه آدرس را مشخص نمایید.



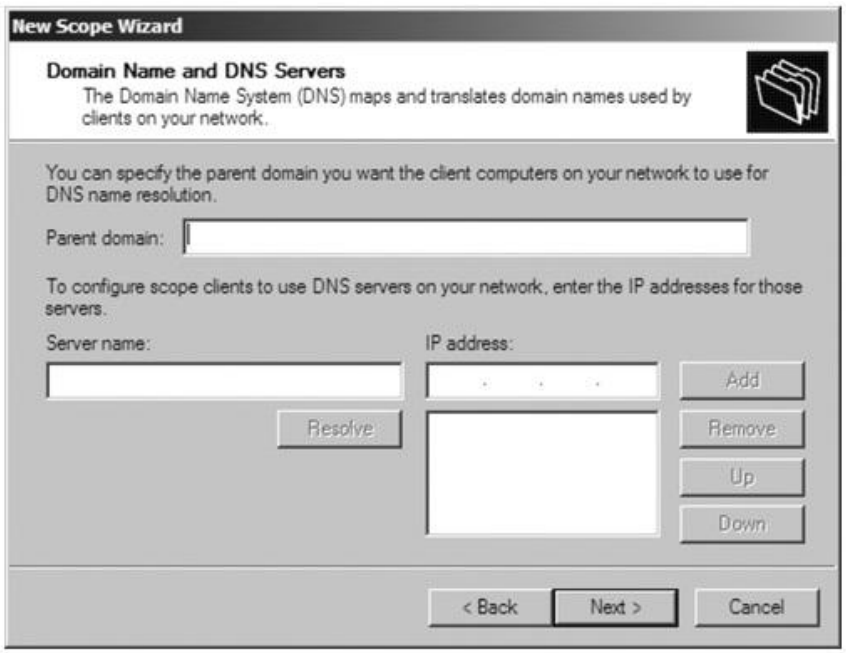
۸. در صفحه Configure DHCP Options از شما سوال می شود که آیا مایل هستید تنظیماتی مثل Default gateways, DNS server and WINS را هم اکنون انجام دهید یا بعد از نصب. ما گزینه "Yes, I want to configure these options now," را انتخاب می کنیم تا روی هر کدام بحث کنیم. کلید Next را بزنید تا به صفحه بعد برویم.



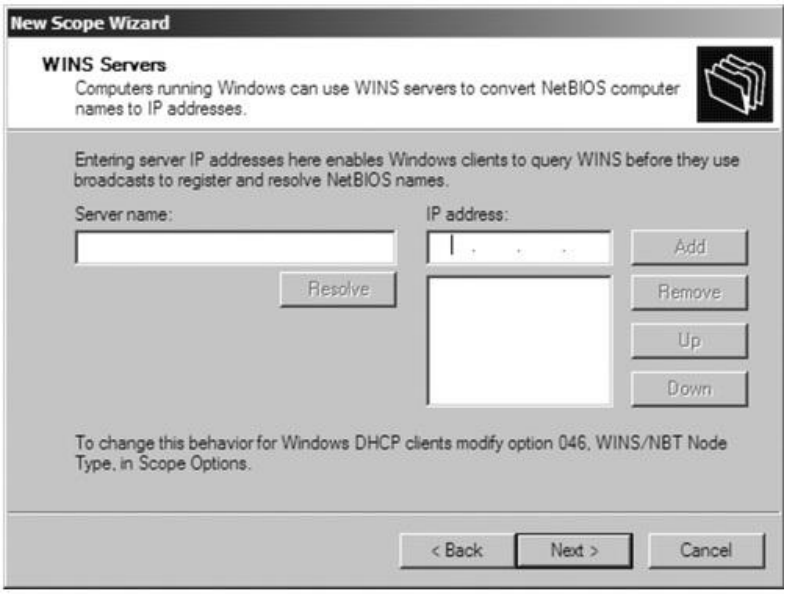
۹. صفحه Router (Default Gateway) نمایان می شود. اینجا شما می توانید یک لیستی از Router ها و یا Gateway های شبکه خود را مشخص کنید. با استفاده از کلید Add می توانید آدرس مورد نظر را اضافه کرده و در صورت نیاز با کلید Remove آن را حذف کنید. بعد از پایان کار روی Next کلیک کنید.



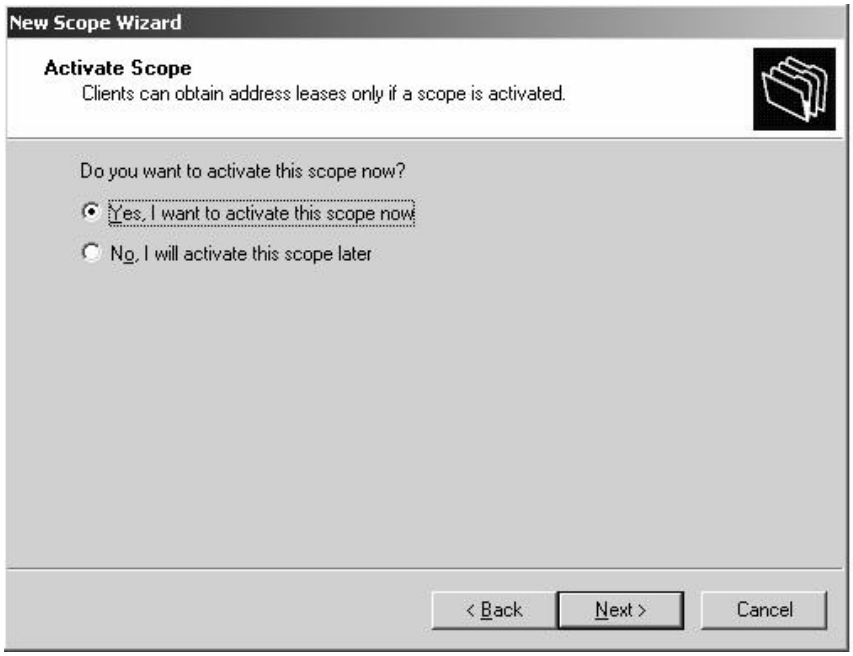
۱۰. صفحه Domain Name and DNS Servers نمایان می شود. همان تور که در تصویر مشاهده می کنید می توان نام دامین مادر و DNS سرور ها را مشخص کرد.



۱۱. صفحه WINS Server نمایان می شود. در این صفحه شما می توانید WINSسرور های سازمان خود را که به کلاینت ها می بایست اختصاص داده شود را وارد کنید. بعد از پایان روی Next کلیک کنید.



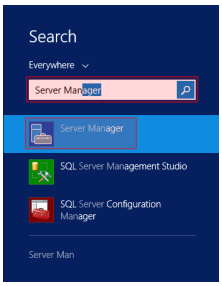
۱۲. سر انجام صفحه فعال سازی Scope نمایان می شود. وقتی شما یک Scope را Active کنید، سرویس DHCP فعال می شود.



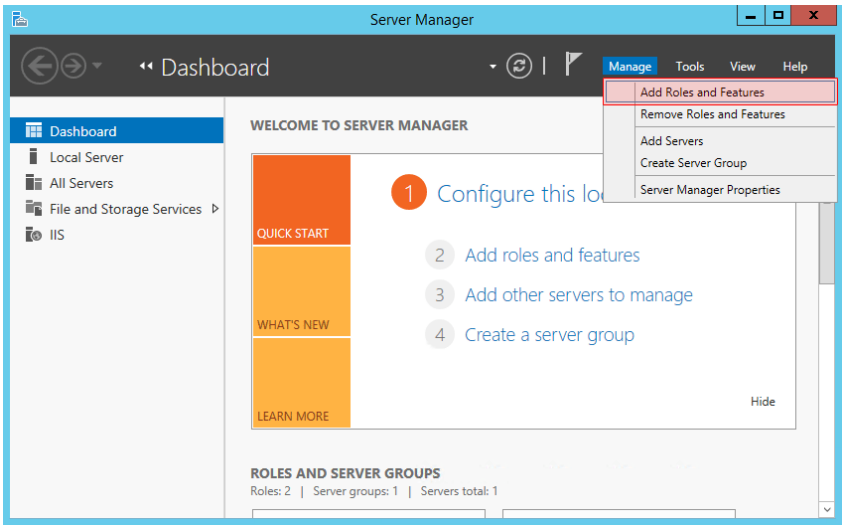
بعد از نصب می توانید کنسول DHCP را از Administrator Tools<pan اجرا کنید. در این کنسول چند عمل مدیریتی دیگر را می توانید انجام دهید که اگر مجالی بود در آینده خواهم نوشت.

DNS

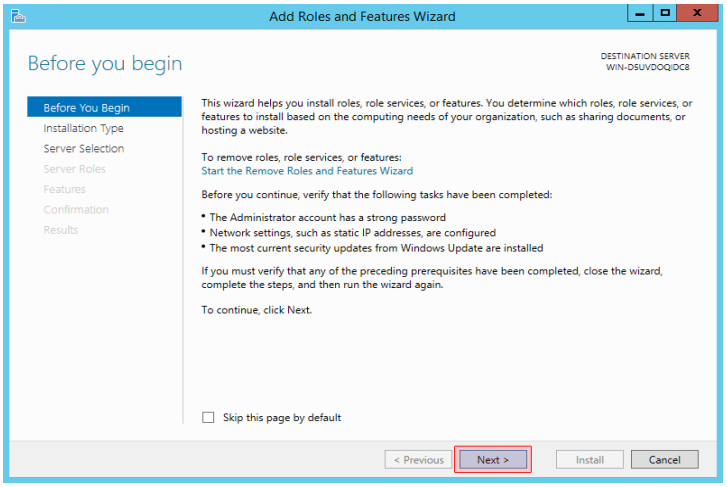
برای شروع در جعبه متن جستجوی ویندوز، عبارت Server Manager را تایپ کنید و در نتایج جستجو بر روی آن کلیک کنید.



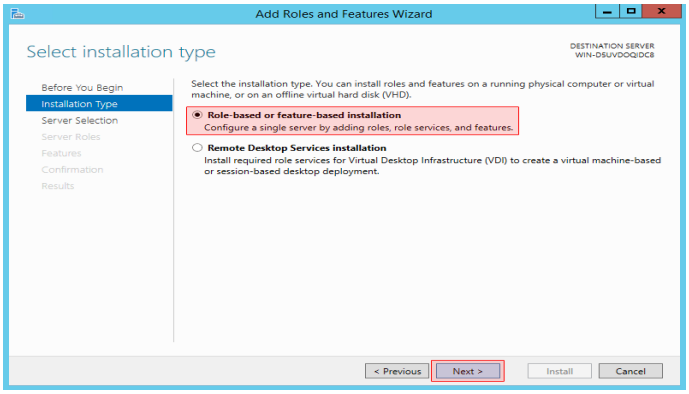
از منوی Manage بر روی گزینه ی Add Roles and Features کلیک کنید.



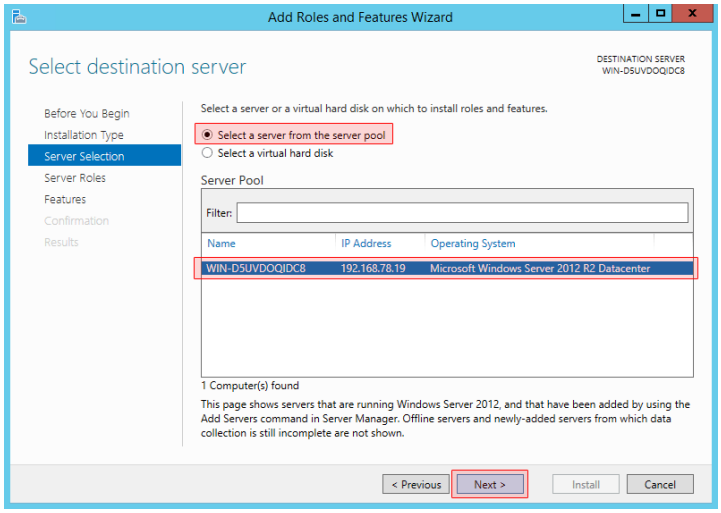
در پنجره باز شده بر روی دکمه ی Next کلیک کنید.



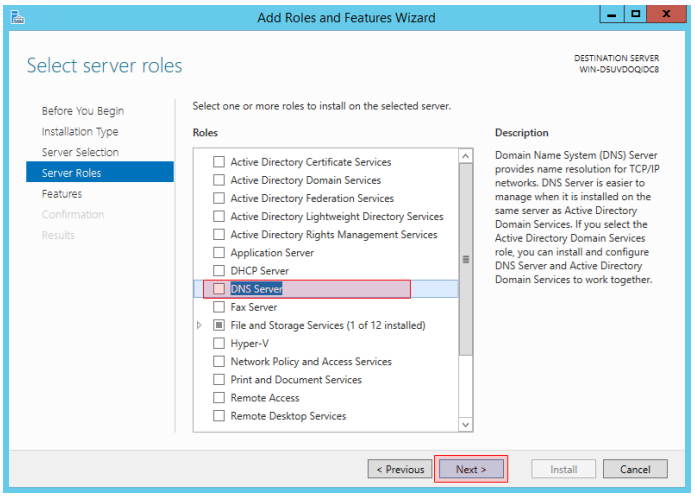
گزینه ی Role-based or feature-based installation را انتخاب کنید و بر روی دکمه ی Next کلیک کنید.



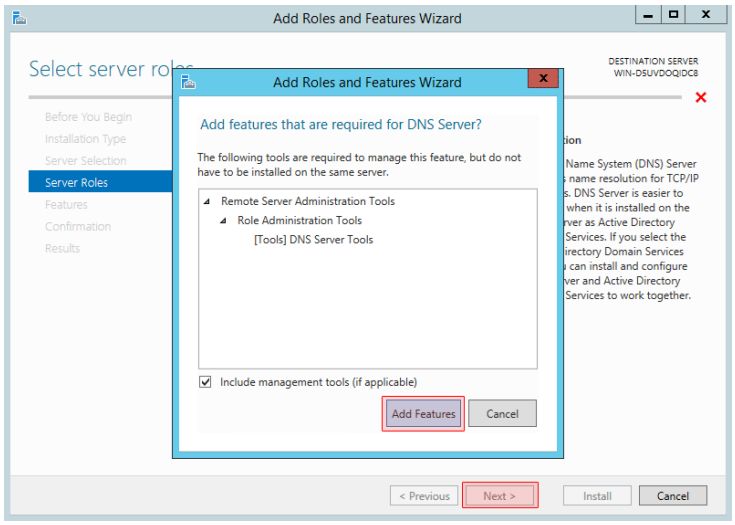
گزینه ی Select a server from the server pool را انتخاب کنید و از لیست سرورهای موجود ، سرور جاری را انتخاب کنید و بر روی دکمه ی Next کلیک کنید.



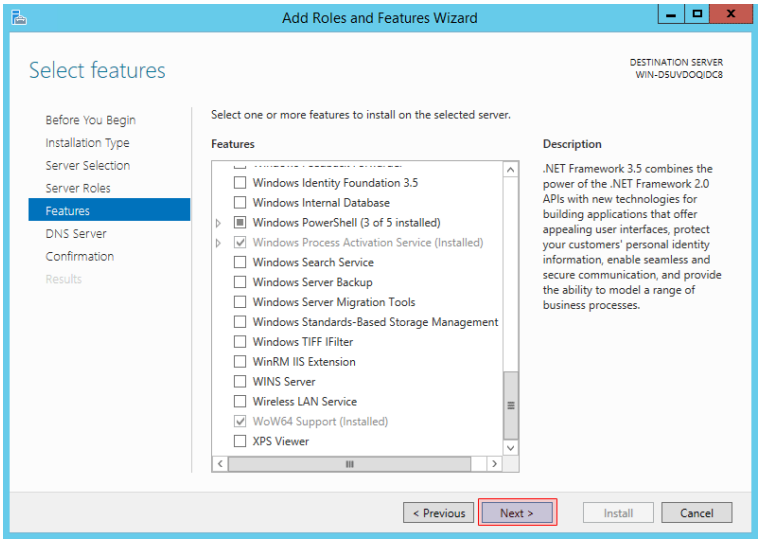
از لیست امکانات موجود گزینه ی DNS Server را تیک بزنید.



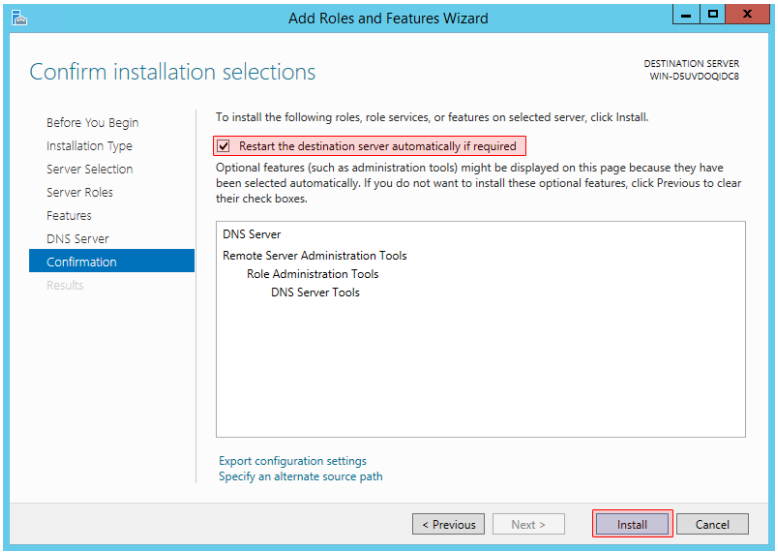
در پنجره ی باز شده بر روی دکمه ی Add Features کلیک کنید و دکمه ی Next را کلیک کنید.



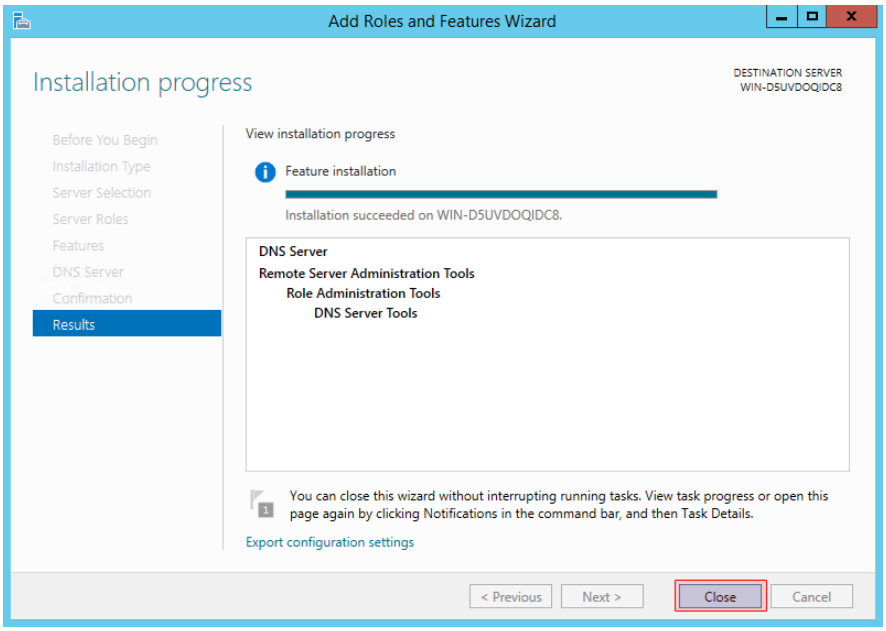
بر روی دکمه ی Next کلیک کنید.



گزینه ی Restart the destination server automatically if required تیک بزنید و بر روی دکمه ی Install کلیک کنید.



بر روی دکمه ی Close کلیک کنید.



نصب DNS Server انجام شد و در این مرحله باید این سرویس رو کانفیگ کنیم.

قبل از شروع شما به یک دامنه نیاز دارید تا Name Server های خودتان را بر روی آن قرار بدهید. به طور مثال اگر دامنه ی mycompany.com متعلق به ما باشد قصد داریم ns1.mycompany.com و ns2.mycompany.com را به عنوان آدرس DNS Server خودمان تعیین کنیم و به مشتریان بدهیم

نکته ی ۱:

دقت کنید که خود دامنه ی company.com هم مثل هر دامنه ی دیگری باید بر روی یک DNS Server تعریف بشود تا به سرور ما اشاره کند. این سرور نمی تواند سرور فعلی ما باشد. در واقع دامنه ی mycompany.com را نمی توانیم بر روی DNS Serverخودمان تعریف کنیم و بعد آدرس ns1.mycompany.com را به عنوان آدرس Name Server آن تعیین کنیم. دلیل این مطلب هم بسیار ساده است. فرض کنید قصد دارید دامنه ی mycompany.com را حل کنید و آدرس آی پی آنرا پیدا کنید. در سرور های ریشه ذکر شده که Name Server این دامنه بر روی آدرس ns1.mycompany.com قرار دارد. بنابراین ابتدا باید ns1.mycompany.com را حل کنیم تا آی پی Name Server را به دست بیاریم. اما برای حل کردن ns1.mycompanyباید mycompany.com را حل کنیم .

چاره این است که DNS Record های مورد نظر شما توسط یک سرور ثالث میزبانی بشود. اکثر فروشندگان سرور مجازی چند DNS Entry را برای این منظور در اختیار شما قرار میدهند. در برخی از سرویس دهندگان دامنه معتبر مثل Tucows بخشی وجود دارد که مخصوص همین کار هست ،

و می توانید آی پی Name Server را هم مستقیما وارد کنید و دیگه نیازی به نگهداری دامنه بر روی یک Name Server ثالث را ندارید.

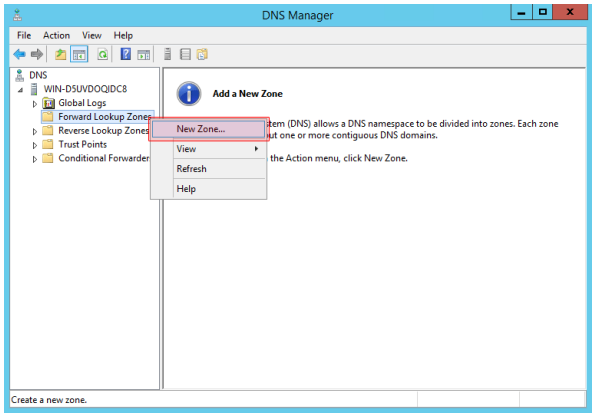
در صورتی که از حالت اول (نگهداری دامنه بر روی Name Server ثالث)استفاده می کنید دو رکورد از نوع A و با نام های ns1و ns2 ایجاد کنید و آنها را به سرور فعلی خودتان که قصد راه اندازی DNS Server بر روی آن دارید ارجاع بدهید.

نکته ی ۲:

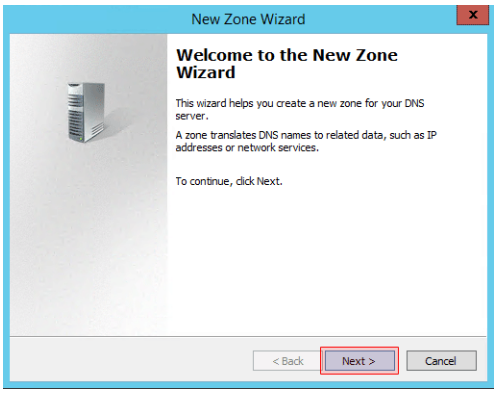
به صورت استاندارد نیاز به حداقل دو Name Sevre مجزا و بر روی دو سرور فیزیکی مجزا با آدرس های مجزا دارید. این یک استاندارد است. اما از آنجایی که ما یک سرور بیشتر در اختیار نداریم هر دو آدرس ns1 و ns2 را بر روی سرور فعلی خودمان ست می کنیم.

توجه: در صورتی که از Name Server ثالث جهت نگهداری Zone مورد نظر (mycompany.com)استفاده می کنید نیازی به انجام تنظیمات این قسمت تا رسیدن به کانفیگ Website Panel نیست.

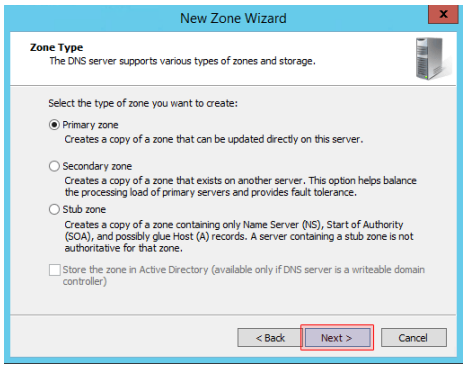
به هر حال با فرض این که دامنه ی mycompany.com را خریداری کرده ایم و تنظیمات DNS آن را هم انجام داده ایم و درحال حاضر به سرور ما متصل هست کار رو شروع می کنیم.
در جعبه ی جستجوی ویندوز عبارت DNS رو تایپ کنید و از لیست جستجو کلیک کنید.
در پنجره ی باز شده از زیر شاخه های سرور مورد نظر بر روی پوشه ی Forward Lookup Zone راست کلیک کنید و گزینه یNew Zone را کلیک کنید.



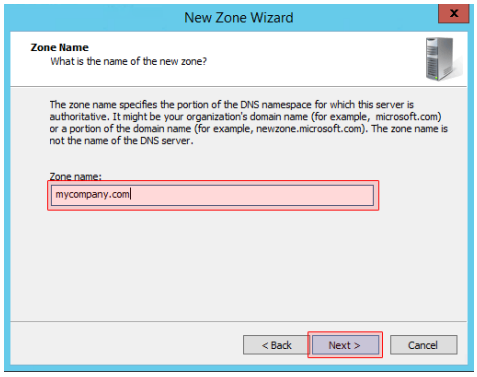
در پنجره ی باز شده بر روی دکمه ی Next کلیک کنید.



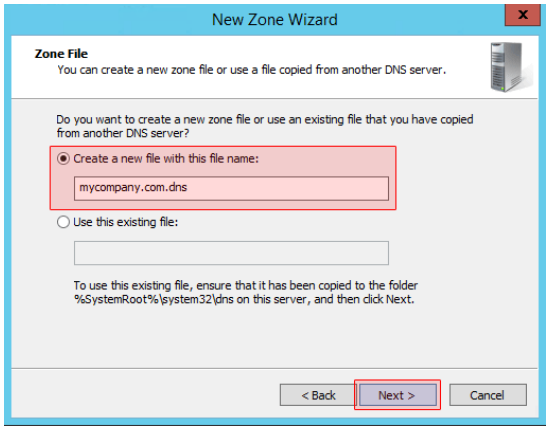
گزینه ی Primary zone را انتخاب کنید و بر روی دکمه ی Next کلیک کنید.



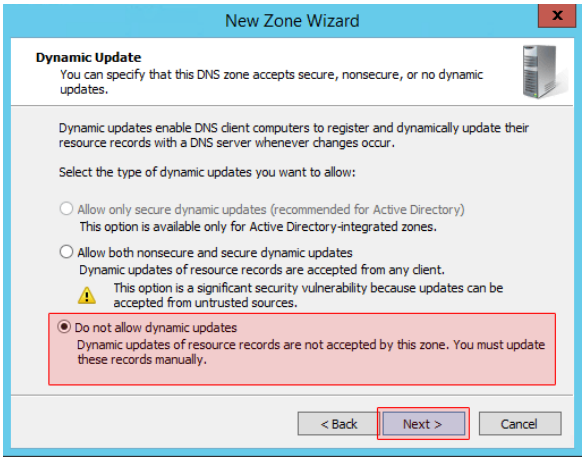
در قسمت Zone name نام دامنه ی مورد نظر خودتان مثلا(mycompany.com) را وارد کنید و بر روی دکمه ی Next کلیک کنید.



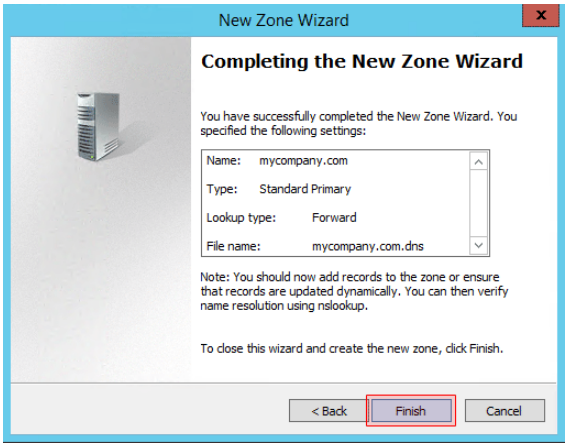
تنظیمات را مطابق شکل زیر قرار بدهید و دکمه ی Next را کلیک کنید.



گزینه ی Do not allow dynamic updates را انتخاب کنید و بر روی دکمه ی Next کلیک کنید.

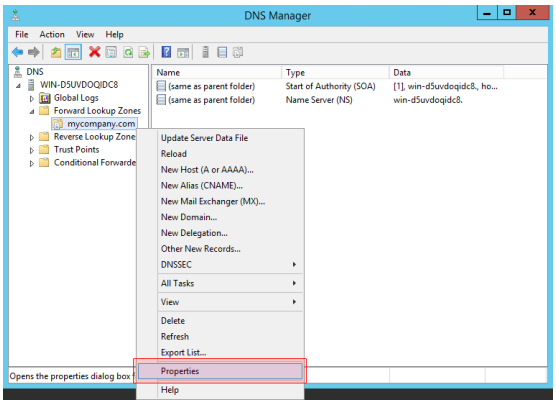


بر روی دکمه ی Finish کلیک کنید.

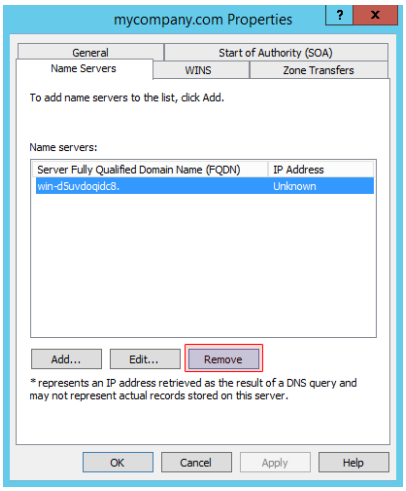


حالا نوبت به کانفیگ Zone مورد نظر هست.

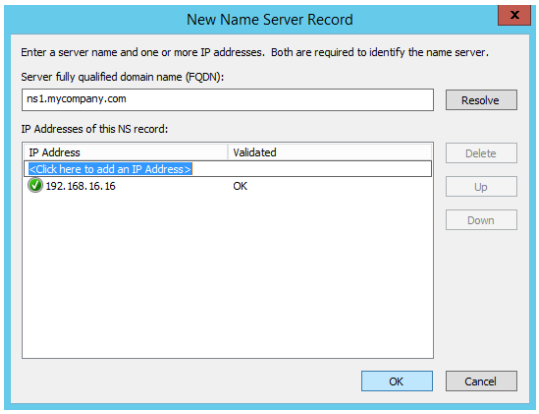
بر روی Zone مورد نظر در اینجا(mycompany.com) کلیک راست کنید و گزینه ی Properties را کلیک کنید.



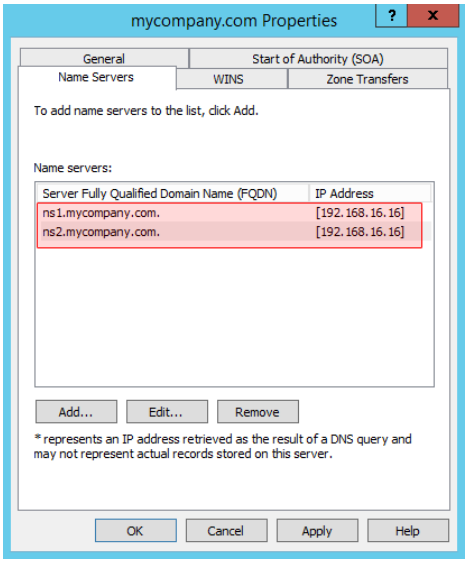
در پنجره ی باز شده به تب Name Servers بروید و Name Server های پیش فرض را حذف کنید و سپس بر روی دکمه ی Addکلیک کنید.



در پنجره ی باز شده آدرس های DNS مورد نظر خودتان به طور مثال(ns1.mycompany.com) و همینطور آی پی سرور را هم وارد کنید و دکمه ی OK رو کلیک کنید.

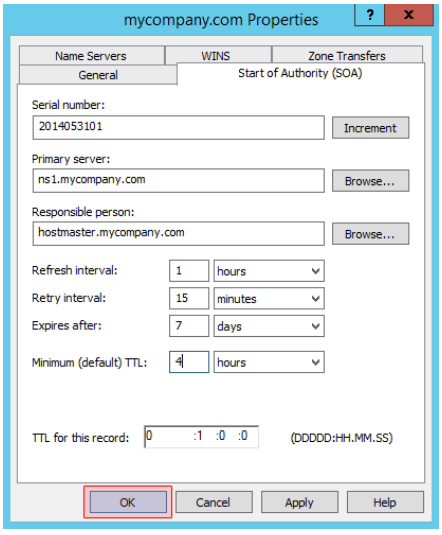


در اینجا ما دو آدرس را انتخاب کردیم.



حالا روی تب Start of Authority (SOA) کلیک کنید و در قسمت Serial number تاریخ فعلی سیستم را به شکل YYYYMMDDNNوارد کنید. در اینجا YYYY سال میلادی، MMماه میلادی، DDروز میلادی و NN مقدار ۰۱ هست. به طور مثال تاریخ 7/05/2016هست و مقدار Serial number را باید ۲۰۱۴۰۵۳۱۰۱ قرار بدهید. در قسمت Primary server یکی از Name Server های خودتان را به عنوان سرور اصلی تعیین کنید.

بقیه موارد را هم مطابق شکل تنظیم کنید و بر روی دکمه ی OK کلیک کنید.



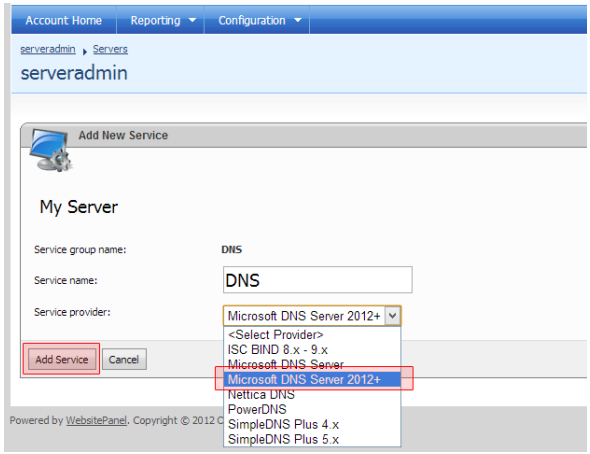
حالا DNS Server شما آماده هست و آدرس های مورد نظر هم بهش اختصاص داده شده (ns1.mycompany.com و ns2.mycompany.com)

نوبت به کانفیگ Website Panel است.

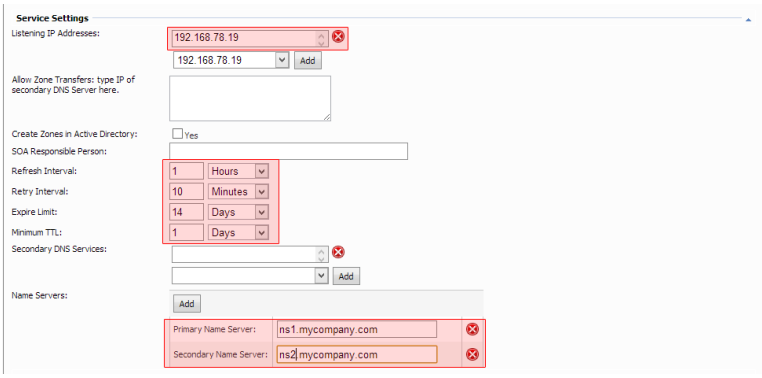
در صورتی که از یک Name Server ثالث جهت نگهداری دامنه اصلی استفاده می کنید نیازی به مراحل بالا ندارید و کار را از اینجا ادامه میدهید.

وارد کنترل پنل خودتان بشوید و از منوی Configuration بر روی گزینه ی Servers کلیک کنید. بر روی عنوان سرور مورد نظر خودتان کلیک کنید. و در صفحه ی باز شده از لیست سرویس ها دکمه ی Add در مقابل DNS رو کلیک کنید.

در صفحه ی باز شده از لیست کشویی گزینه ی Microsoft DNS Server 2012 را انتخاب کنید و روی دکمه ی Add Serviceکلیک کنید.



در صفحه ای که باز شده تنظیمات را مطابق با شکل زیر قرار بدهید و بر روی دکمه ی Update کلیک کنید.



سرویس DNS شما آماده ی استفاده هست.

کاربرد حوزه ها

برای تحلیل یک نام حوزه، سطوح از سمت راست به چپ تفکیک می‌شوند و در یک روند سلسله مراتبی، سرویس دهندهٔ متناظر با آن سطح پیدا می‌شود.

نام‌های حوزه به هفت منطقهٔ عمومی و حدود صد و اندی منطقهٔ کشوری تقسیم بندی شده‌است. حوزه بدین معناست که شما با یک نگاه ساده به انتهای نشانی نمادین، می‌توانید ماهیت آن نام و سرویس دهندهٔ متناظر با آن را حدس بزنید. یعنی اگر انتهای نام‌های حوزه متفاوت باشد منطقهٔ جستجو برای یافتن نشانی آی‌پی معادل نیز متفاوت خواهد بود.

هفت حوزه ی عمومی که همه آنها سه حرفی هستند عبارتند از:

- .comصاحب این نام جزو موسسات اقتصادی و تجاری به شمار می‌آید.
- .eduصاحب این نام جزو موسسات علمی یا دانشگاهی به شمار می‌آید.
- .govاین مجموعه از نام‌ها برای آژانس‌های دولتی آمریکا اختصاص داده شده‌است.
- .intصاحب این نام یکی از سازمان‌های بین‌المللی (مثل یونسکو، فائو، ...) است.
- .milصاحب این نام یکی از سازمان‌های نظامی دنیا به شمار می‌آید.
- .netصاحب این نام جزو یکی از «ارائه دهندگان خدمات شبکه» به شمار می‌رود.
- .orgصاحب این نام جزو یکی از سازمان‌های غیر انتفاعی محسوب می‌شوند.

نام‌های حوزهٔ بسیار زیادی در اینترنت تعریف شده‌اند که هیچیک از حوزه‌های سه حرفی هفتگانه را در انتهای آنها نمی‌بینید. معمولاً در انتهای این نشانی‌ها یک رشتهٔ دو حرفی مخفف نام کشوری است که آن نشانی و ماشین صاحب آن، در آن کشور واقع است.

هر حوزه می‌تواند به زیر حوزه‌های کوچکتری تقسیم شود، که به آن دامنه ی سطح دوم نیز گفته می شود.

به عنوان مثال، نام های مربوط به حوزه ایران، که با مخفف .ir مشخص می شود، به ۷ زیرحوزه، به شرح زیر تقسیم می شود:

- .ac.ir : فقط برای دانشگاه‌ها یا موسسه های آموزشی
- .co.ir : فقط برای شرکت های سهامی خاص ، سهامی عام، مسوولیت محدود و تضامنی
- .gov.ir : فقط برای موسسه ها یا سازمان های دولتی
- .id.ir : فقط برای افراد دارای ملیت ایرانی
- .net.ir : فقط برای سرویس دهندگان رسمی اینترنت
- .org.ir : فقط برای موسسه ها و سازمان های خصوصی
- .sch.ir : فقط برای مدارس

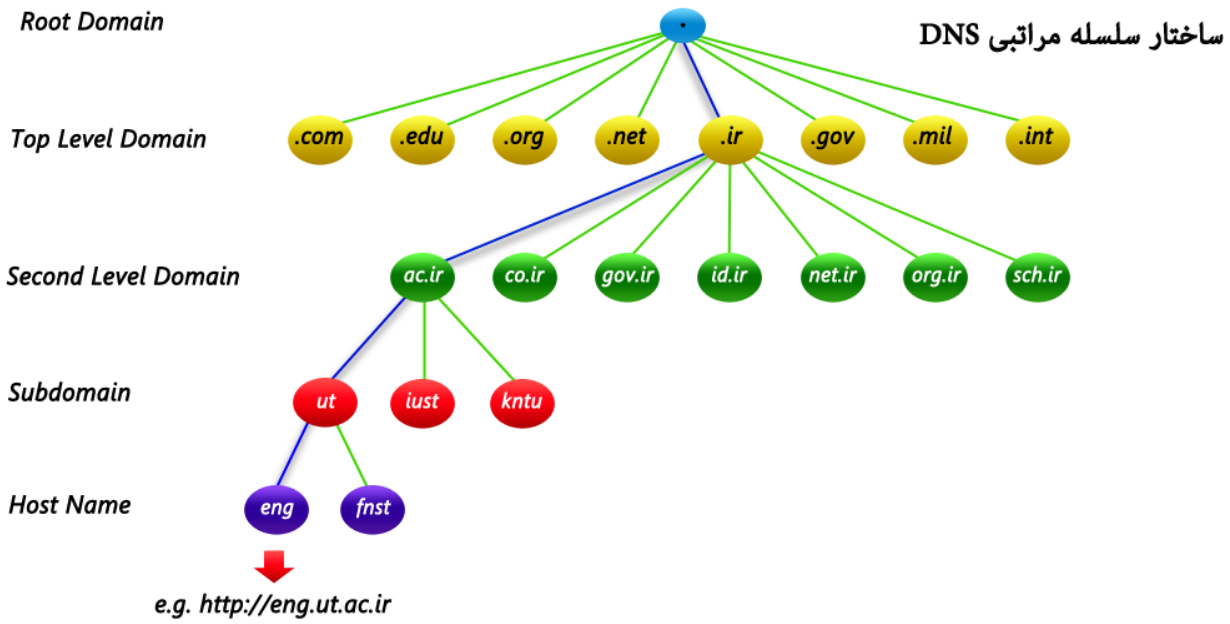
بعنوان مثال http://eng.ut.ac.ir :

- کشور : ایران
- هویت : دانشگاه
- نام دانشگاه ut : مخففی برای نام دانشگاه تهران
- نام دانشکده eng : مخففی برای بخش فنی مهندسی

حوزه‌ها با دامنه‌ها یکسان نبوده و یک حوزه می‌تواند شامل مقادیری در رابطه با چندین دامنه باشد.

برفرض، دامنه www.google.com دارای زیردامنه ای به نام news است(news.google.com) ،

درصورتیکه زیردامنه mail آن (mail.google.com) از دامنه اختصاصی www.gmail.com نیز قابل دسترسی می باشد



روش های جست جو

همانگونه که اشاره شد، اسامی نمادین در شبکه اینترنت که خود در قالب حوزه‌ها و زیر حوزه‌ها سازماندهی شده‌اند، در یک فایل متمرکز ذخیره نمی‌شوند بلکه روی کل شبکه اینترنت توزیع شده‌اند، به همین دلیل برای ترجمه یک نام به نشانی آی‌پی ممکن است چندین مرحله «پرس و جو» صورت بگیرد تا یک نشانی پیدا شود.

طبیعی است که یک پرس و جو برای تبدیل یک نام حوزه همیشه موفقیت آمیز نباشد و ممکن است به پرس و جوهای بیشتری نیاز شود یا حتی ممکن است یک نشانی نمادین اشتباه باشد و هیچ معادل نشانی آی‌پی نداشته باشد.

سه روش برای پرس و جوی نام در سرویس دهنده‌های نام وجود دارد:

- پرس و جوی تکراری
- پرس و جوی بازگشتی
- پرس و جوی معکوس

پرس و جوی تکراری

در پرس و جوی تکراری قسمت اعظم تلاش برای تبدیل یک نام بر عهده سرویس دهنده محلی است؛ این DNS حداقل به نشانی ماشینRoot ، به عنوان نقطه شروع نیاز دارد. وقتی یک تقاضای ترجمه نشانی به سرویس دهنده محلی ارسال می‌شود در صورتی که قادر به ترجمه نام به معادل نشانی آی‌پی آن باشد، معادل نشانی آی‌پی نام مورد نظر را به تقاضا کننده برمی گرداند. (این حالت

وقتی است که سرویس دهنده محلی قبلاً آن نام را ترجمه و در یک فایل ذخیره کرده باشد.) در غیر این صورت سرویس دهنده محلی خودش یک تقاضا برای DNS سطح بالا ارسال می‌کند. این سرویس دهنده، نشانی ماشینی را که می‌تواند برای ترجمه نام مورد نظر مفید باشد، به سرویس دهنده محلی معرفی می‌کند؛ سرویس دهنده محلی مجدداً یک تقاضا به ماشین معرفی شده در مرحله قبل ارسال می‌کند.

در این حالت هم سرویس دهنده نام می‌تواند در صورت یافتن نشانی آی‌پی با آن نام حوزه، آنرا ترجمه کند و یا آنکه نشانی سرویس دهنده سطح پایینتری را به او برگرداند.

این روند ادامه می‌یابد تا DNS نهایی نام مورد نظر را به نشانی آی‌پی ترجمه نماید. برای درک بهتر از روند کار به شکل زیر دقت کنید. در این مثال فرض شده‌است که یک برنامه ی کاربردی با فراخوانی «تابع تحلیلگر نام»، تقاضای ترجمه نام www.microsoft.comرا می‌نماید. مراحلی که انجام می‌شود به شرح زیر است:

- در مرحله اول برنامه کاربردی با فراخوانی «تابع تحلیل نام»، تقاضای ترجمه نشانی www.microsoft.com را برای سرویس دهنده محلی ارسال کرده و منتظر می‌ماند.
- در مرحله دوم، سرویس دهنده محلی از سرویس دهنده) Root که حوزه‌های متفاوت را تفکیک می‌کند) نشانی ماشین یک DNS که متولی حوزه com.است را سؤال می‌کند.
- در مرحله سوم، نشانی سرویس دهنده مربوط به حوزه com .بر می‌گردد.
- در مرحله چهارم، سرویس دهنده محلی، از ماشین معرفی شده در مرحله قبلی، نشانی سرویس دهنده مربوط به حوزه Microsoft.comرا سؤال می‌نماید.
- در مرحله پنجم فهرستی از سرویس دهنده‌های DNS مربوط به Microsoft.com بر می‌گردد.
- در مرحله ششم، سرویس دهنده محلی تقاضای ترجمه نشانی نمادین www.microsoft.com را از DNS متعلق به حوزه Microsoft.com می‌کند.
- در مرحله هفتم، معادل نشانی آی‌پی نام www.microsoft.com برمی گردد.
- در مرحله هشتم، نشانی آی‌پی خواسته شده در اختیار برنامه کاربردی قرار می‌گیرد.

جست و جوی بازگشتی

در این روش هر گاه برنامه‌ای بخواهد نشانی آی‌پی معادل یک نام مثل cs.yale.edu را بدست آورد، بگونه‌ای که قبلاً اشاره شد، «تابع سیستمی تحلیل نام» را فراخوانی می‌کند. این تابع یک ماشین را بعنوان سرویس دهنده محلی از قبل می‌شناسد و بنابراین تقاضای تبدیل نام را به روش UDP برای آن ارسال کرده و منتظر جواب می‌ماند (پاسخ نهایی DNS طبیعتاً باید یک نشانی ۳۲ بیتی معادل نشانی آی‌پی یک ماشین باشد)

دو حالت ممکن است اتفاق بیفتد

ممکن است در بانک اطلاعاتی مربوط به سرویس دهنده محلی، نشانی آی‌پی معادل با آن نام از قبل وجود داشته و بالطبع به سرعت مقدار معادل نشانی آی‌پی آن بر می‌گردد.

ممکن است در بانک اطلاعاتی سرویس دهنده محلی، معادل نشانی آی‌پی آن نام وجود نداشته باشد. مثلاً سرویس دهنده محلی در بانک اطلاعاتی خودش معادل نشانی آی‌پی نام cs.mit.edu را نداشته و طبیعتاً نمی‌تواند آن را ترجمه کند.

در چنین حالتی سرویس دهنده محلی موظف است بدون آنکه به تقاضا دهنده خبر بدهد، خودش رأساً به سرویس دهنده سطح بالاتر تقاضای ترجمه نشانی بدهد. در این حالت هم DNS سطح بالاتر به همین نحو، ترجمه نشانی را پیگیری می‌کند. یعنی اگر معادل نشانی آی‌پی آن نام را داشته باشد آنرا برمی گرداند و در غیر اینصورت خودش از سرویس دهنده سطح پایینتر تقاضای ترجمه آن نام را می‌نماید و این مراحل تکرار می‌شود. در روش پرس و جوی بازگشتی ماشین سرویس دهنده محلی این مراحل متوالی را نمی‌بیند و هیچ کاری جز ارسال تقاضای ترجمه یک نشانی بر عهده ندارد و پس از ارسال تقاضا برای سرویس دهنده سطح بالا منتظر خواهد ماند.

بازهم تکرار می‌کنیم، روشی که DNS برای ترجمه نشانی بکار می‌برد می‌تواند بدون اتصال (UDP) باشد که این کار به سرعت عمل ترجمه نشانی می‌افزاید.

دقت کنید که در روش پرس و جوی تکراری نسبت به روش پرس و جوی بازگشتی، حجم عمده عملیات بر عهده سرویس دهنده DNSمحلی است و مدیریت خطاها و پیگیری روند کار ساده تر خواهد بود و روش منطقی تری برای بکارگیری در شبکه اینترنت محسوب می‌شود. روش پرس و جوی بازگشتی برای شبکه‌های کوچک کاربرد دارد. برای درک بیشتر این روش به شکل زیر دقت کنید.

پرس و جوی معکوس

فرض کنید حالتی بوجود بیاید که یک سرویس دهندهDNS ، نشانی آی‌پی یک ماشین را بداند ولی نام نمادین معادل با آن را نداند. بعنوان مثال DNS مایل است بداند که چه نامی در شبکه اینترنت معادل با ۱۹۵,۱۳,۴۲,۷ می‌باشد.

در چنین حالتی مسئله کمی حادتر به نظر می‌رسد، چرا که برای ترجمه نامهای نمادین، چون این نامها دارای حوزه و زیرحوزه هستند، تحلیل نشانی ها ساده‌است. ولی ترجمه نشانی آی‌پی به معادل نام حوزه، از چنین روابطی تبعیت نمی‌کند؛ بعبارت بهتر هیچ ارتباط مستقیم و متناظری بین نشانی های آی‌پی و اسامی انتخاب شده در اینترنت وجود ندارد. برای یافتن نامهای متناظر با یک نشانی آی‌پی باید یک جستجوی کامل و در عین حال وقت گیر، انجام بشود.

روش کار بدین صورت است که سرویس دهنده محلی یک تقاضا برای DNS متناظر با شبکه‌ای که مشخصه آن در نشانی آی‌پی، مشخص شده، ارسال می‌کند.

بعنوان مثال نشانی آی‌پی شبکه‌ای را ۱۳۸,۱۴,۷,۱۳ در نظر بگیرید، نشانی کلاس B و مشخصه آن ۱۳۸,۱۴,۰,۰ است. زمانی که مؤسسه‌ای یک کلاس نشانی آی‌پی ثبت می‌دهد یک سرویس دهندهDNS ، متناظر با شبکه خود ایجاد کرده و آنرا نیز معرفی می‌کند. سرویس دهنده محلی بایستی نشانی DNS متناظر با شبکه ۱۳۸,۱۴,۰,۰ را پیدا کرده و سپس برای آن یک تقاضا ارسال کند DNS .مربوط به این شبکه، براساس زیر شبکه‌هایی که دارد، این سؤال را از طریق سرویس دهنده‌های متناظر با هر زیر شبکه

پیگیری می‌کند. (چون هر زیر شبکه یک سرویس دهنده DNS مخصوص به خود دارد) نهایتاً یک نام نمادین حوزه معادل با آن نشانی آی‌پی بر خواهد گشت.

معرفی اکتیودایرکتوری

اکتیودایرکتوری بوسیله دامین کنترولر مدیریت میشود . هنگامی که یک دامین کنترلر (Domain controller) را نصب و پیکربندی می کنید، اکتیودایرکتوری تشکیلات بسیاری را برایتان نصب می نماید و به شما امکان ساخت و مدیریت انواع مختلف اشیاء را می دهد. در واقع اکتیودایرکتوری یک پایگاه داده مرکزی است که در آن اشیاء مختلفی از جمله حسابهای کاربری ، حسابهای کامپیوتری ، گروه ها ، OUها و غیره ذخیره می شوند. محتوی اشیاء اکتیو دایرکتوری اطلاعات لازم برای شیء از جمله توصیف ها ، حقوق file system ، شاخص های امنیتی ، حقوق application و اطلاعات پوشه ها را شامل می شود .

شما بعنوان یک مدیر شبکه یکی از مسئولیت های اصلی تان ساخت و پیکربندی کاربران ، گروه ها ، اکانت های کامپیوتر ، واحدهای سازماندهیOU) ها) و group poliy ها می باشد. شبیه به مبحث اکتیودایرکتوری در ورژن های قبلی ویندوز سرور، در ویندوز سرور ۲۰۰۸ نیز اکتیو دایرکتوری از کنسول Active Directory Users and Computers برای مدیریت اکانت های کاربران و گروه ها و کامپیوترها استفاده می کند. در این کنسول علاوه بر کارهای ذکر شده شما می توانید دیگر جنبه های اکتیودایرکتوری شامل group policy ، domain controller، domain security policyو غیره را مدیریت نمایید .

با این کنسول که بیشترین استفاده را در وظایف مدیریتی روزانه در ساختار اکتیودایرکتوری دارا می باشد ، برای ایجاد ، مدیریت و نگهداری و همچنین حذف حسابهای کامپیوتری و کاربری در اکتیودایرکتوری استفاده می شود. باید توجه کرد که اشیاء در اکتیو دایرکتوری به شکل تودرتو در گروه هایی که واحد های سازماندهی (OU) نامیده می شوند قرار می گیرند. بسیاری از وظایفی که توسط کنسول
Active Directory Users and Computersانجام می شود شامل موارد زیر می باشد :

۱. اضافه کردن کاربر جدید در اکتیو دایرکتوری
۲. تغییر پسوردهای کاربران
۳. واگذاری حقوق خاصی به فایل سرورها
۴. اجازه remote access به شبکه
۵. تنظیم login and logout script ها
۶. ساختن گروه های امنیتی(security groups)

بسیاری از برنامه شامل Exchange Server ، Terminal Servicesو System Center توانایی اضافه شدن به اکتیو دایرکتوری در بسیاری از مواقع را دارند. این برنامه ها به اکتیو دایرکتوری اجازه مدیریت اشیاء وابسته به خود را می دهند . برای

مثال اگر برنامه Terminal Services را به شبکه تان اضافه می کنید ، شما می توانید از طریق کنسول Active Directory Users and Computersمدت زمان اتصال هر کاربر به شبکه را کنترل نمایید .

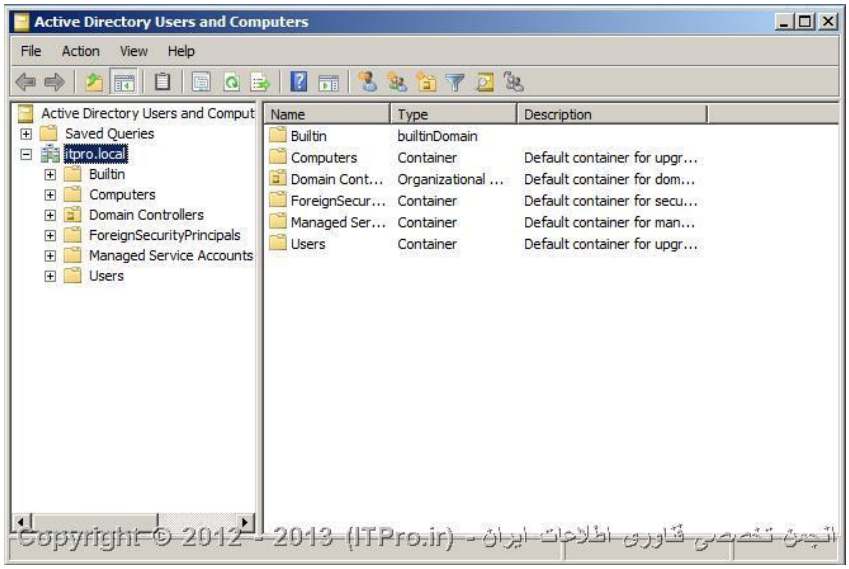
شما می توانید برای دسترسی به کنسول Active Directory Users and Computers از مسیرهای زیر استفاده کنید :

دقت کنید که فقط Domain Controller ها دارای چنین کنسولی هستند و اگر نتوانستید این کنسول را بیابید ، مطمئن شوید که بر روی دامین کنترولر login کرده اید .

Start --> Programs --> Administrative Tools Active Directory Users and Computers

Start --> Control Panel --> Administrative Tools Active Directory Users and Computers

بعد از آشنایی با طریقه دسترسی به Active Directory Users and Computers ، حالا وقت آنست که container ها و OUهای پیش فرض بطور مختصر مورد بررسی قرار گیرند. بعد از نصب و پیکربندی Domain controller ، به طور پیش فرض شما چندین container و OU ی توکار را در کنسول Active Directory Users and Computers مانند (تصویر ۱) می بینید.ساختار اکتیودایرکتوری بر اساس forest است که هر Forest می تواند دارای چندین Domain و یا Tree باشد .کنسول Active Directory Users and Computersبه شما اجازه کار کردن با ساختار Forest را نمی دهد و شما می توانید فقط ساختار Domain را با آن مدیریت کنید .



تصویر ۱

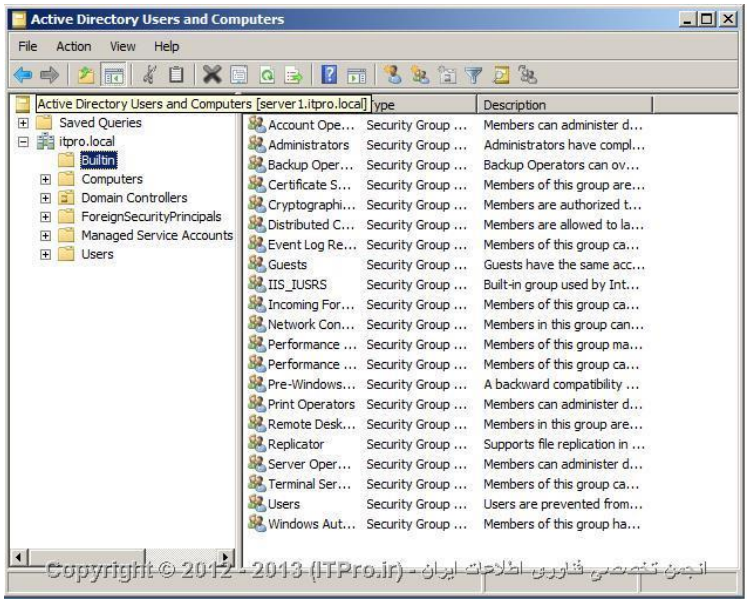
اگر به (تصویر ۱) نگاه کنید می بینید که itpro.local دامینی است که در شبکه من وجود دارد . تمامی اشیائی که در ساختار اکتیودایرکتوری من ساخته می شوند عضوی از دامین itpro.local هستند. اما این تنها دامینی نیست که در شبکه من وجود دارد. کنسول Active Directory Users and Computers برای اینکه در کار مدیریتی دامین ها پیچیدگی و ابهامی پیش نیاید در هر لحظه فقط یکی از دامین ها را به ما نشان می دهد . دامینی که در اولین صفحه این کنسول مشاهده می کنیم در حقیقت همان دامینی است که متعلق به Domain controller ای است که به آن loginکرده ایم . یعنی در اینجا ما بر روی

دامین کنترلری login کرده ایم که دامین itpro.local بر روی آن قرار دارد .

اما مشکل در اینجاست که دامین ها ممکن است بصورت فیزیکی و جغرافیایی از هم فاصله داشته باشند . برای مثال بسیاری از شرکت ها وجود دارند که دارای نمایندگی هایی در مناطق مختلف هستند و برای هر کدام از این مناطق نیز یک دامین دارند و شما برای اینکه بتوانید به هر کدام از این دامین ها دسترسی داشته باشید نیاز به یک ابزار دارید. شما میتوانید از طریق کنسول Active Directory Users and Computersبه دامین هایی که به آنها اعتماد و دسترسی لازم را دارید نیز دسترسی پیدا کنید . تمام کاری که باید بکنید این است که بر روی دامین مورد نظر کلیک راست کرده و گزینه Connect To Domain را بزنید . صفحه ای برای شما باز خواهد شد که به شما این امکان را می دهد که بتوانید نام دامین مورد نظرتان را در آن تایپ کرده و یا اینکه دامین مورد نظرتان را از لیست انتخاب کنید . و براحتی با گزینه Browse دامین مورد نظر برای شما باز خواهد شد .

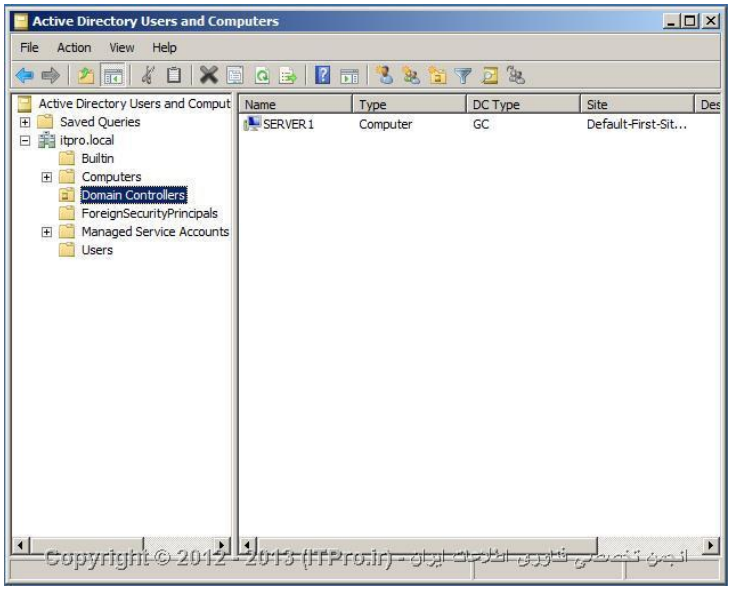
در (تصویر ۱) شما تعدادی Container را مشاهده می کنید که هرکدام به نوعی از اشیاء اشاره میکنند . هر شیئی که در اکتیودایرکتوری ساخته می شود به یک Object Typeمرتبط می شود که در این ساختار به آنها کلاس شیء یا Object Class هم گفته می شود . همچنین هر شیء برای خود یک سری خواص یا Attribute دارد که به آن مرتبط شده اند که این خواص بسته به نوع اشیاء متفاوت هستند. پس بعد از نصب و پیکربندی یک دامین کنترولر چندین بخش سازماندهی (Container) را درون کنسول Active Directory Users and Computers می بینید که به قرار زیر می باشند:(شبیه به Folder هستند)

Built-In : شامل همه گروه های امنیتی پیش فرضی می باشد که به هنگام نصب دامین کنترولر به صورت خودکار ساخته می شوند. این گروه ها مجوزهای استانداردی را بر روی اشیاء مختلف درون اکتیودایرکتوری می گذارند . این Container شامل گروه های Account Operators group, Administrators , Users Backup Operators, Server Operators, Replicators, Users, Remote Desktopو Print Operators می شود .



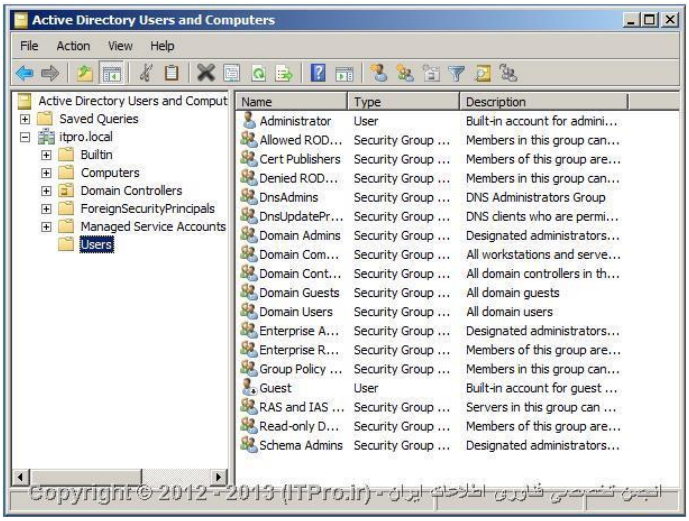
Computers : شامل ایستگاهای کاری درون دامین تان می شود. به طور پیش فرض هیچ ایستگاه کاری درون این containerوجود ندارد، اما با پیوستن یک ایستگاه کاری به دامین تان شما می توانید آن کامپیوتر را درون این container مشاهده کنید .

Domain Controllers : شامل همه دامین کنترول هایی است که دامین شما را کنترل می نمایند .



Foreign Security Principals : این container همه اشیائی که بخشی از دامین تان نمی باشند را در خود نگه می دارد و مجوزهایی که باید به کار ببرند را به آنها اختصاص می دهد .

Users : شامل همه اکانت های امنیتی است که بخشی از دامین می باشند . چندین گروه در این container وجود دارند که در هنگام نصب دامین کنترولر به صورت خودکار ساخته می شوند . این container شامل اکانت پیش فرض Administrator و گروه هایی مانند Domain Admins ، Enterprise Admins، Domain Controllers، Domain Guests، Domain Users، Schema Admins، Guestsو غیره می باشد .



در ضمن شما می توانید انواع مختلفی از اشیاء اکتیودایرکتوری را ساخته و مدیریت نمایید. بعضی از این اشیاء به قرار زیر می باشند :

Computer : اشیاء کامپیوتر ایستگاه های کاری که بخشی از دامین اکتیو دایرکتوری می باشند را نمایش می دهند . همه کامپیوتر های درون یک Domain در یک پایگاه داده امنیتی یکسان که شامل اطلاعات گروه ها و کاربران می باشد ، سهیم می باشند. اشیاء کامپیوتر برای مدیریت مجوز های امنیتی و محدودیت های enforcing Group Policy مفید می باشند .

Contact : این اشیاء معمولا در OU ها برای مشخص کردن تماس های مدیریتی مورد استفاده قرار می گیرند Contact .ها مسئولیت های امنیتی شبیه به کاربران را ندارند و فقط برای مشخص کردن اطلاعات درباره اشخاص درون سازمان ها مورد استفاده قرار می گیرند .

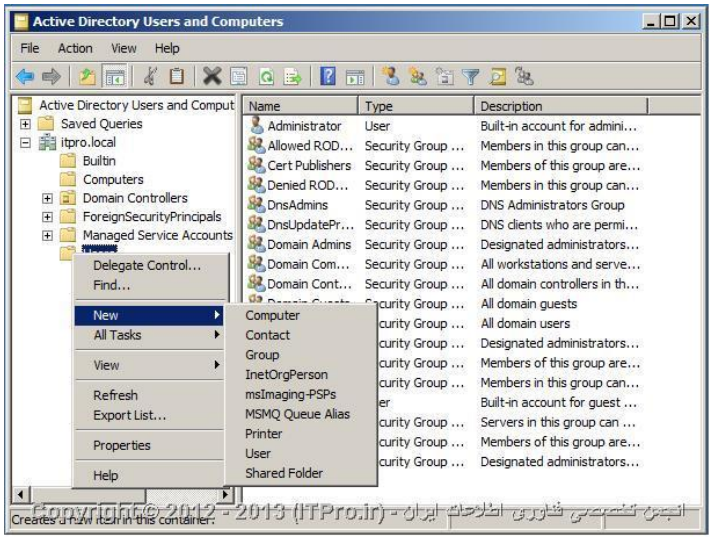
Group : اشیاء گروه، مجموعه هایی منطقی از کاربران اصلی هستند که دسترسی های امنیتی را به منابع اختصاص می دهند. هنگامی که کاربران را مدیریت می کنید ، شما باید آنها را درون گروه ها قرار دهید و سپس مجوزها را به گروه اختصاص دهید. این کار مدیریت انعطاف پذیرتری را بدون نیاز به اختصاص دادن مجوزها بصورت فردی برای کاربر فراهم می آورد .

Organizational Unit : یک شیء OU برای ایجاد یک سلسله مراتب درون دامین اکتیو دایرکتوری مورد استفاده قرار می گیرد. آن کوچکترین واحدی است که برای ساختن گروه های مدیریتی از آن استفاده می شود. و همچنین می توان از آن برای تخصیص سیاست های گروه (group policy) استفاده کرد. به طور معمول ساختار OU درون یک دامین سلسله مراتب سازماندهی یک شرکت تجاری را بازتاب می دهد .

Printer : شیء پرینتر نگاشتی برای دستگاه های پرینتر می باشد .

Shared Folder : این شیء نگاشتی برای server share ها می باشند. آنها برای سازماندهی منابع فایلی مختلفی که ممکن است بر روی file/print server ها موجود باشند مورد استفاده قرار می گیرند. اغلب از اشیاء Shared Folder برای دادن نام منطقی به مجموعه فایل های مشخصی استفاده می شود .

User : یک شیء کاربر مسئول امنیتی بنیادی بر روی اکتیودایرکتوری می باشد. اکانت های کاربر شامل اطلاعاتی در باره اشخاص از قبیل پسورد و دیگر اطلاعات مربوط به مجوز ها می باشد .



اکتیودایرکتوری همچنین میتواند که اطلاعات را با دیگر سرویس های دایرکتوری مثل NOVELL و پروتوکل LDAP را پشتیبانی میکنند و به اشتراک میگذارند .

۱. LDAP : یک استاندارد اینترنتی است که برای دسترسی به سرویس های دایرکتوری توسعه داده شده است و به جهت ساده سازی متناوب دسترسی به دایرکتوری یا همان پروتکل DAP میباشد. همچنین برای تبادل اطلاعات بین دایرکتوری ها از این پروتوکل استفاده میکند.

۲. HTTP : نیز یک پروتوکل استاندارد جهت نمایش صفحات وب میباشد لذا شما میتوانید هر شی داخل مرورگر را به نمایش بگذارید و از فواید اکتیودایرکتوری است که شما میتوانید صفحات وب را با کد HTML به جهت نمایش برای کاربران دراورید. اکتیو دایرکتوری نام های UNC را پشتیبانی میکند نام هایی که در شبکه مبتنی بر ویندوز به درایورهای به اشتراک گذاشته شده و پرینترها و فایل ها مراجعه میکنند.

ساختار اکتیو دایرکتوری

اکتیو دایرکتوری یک روش طراحی ساختار دایرکتوری را برای سازمان شما فراهم میکند.لذا قبل از نصب اکتیو دایرکتوری شما بایستی عملیات و ساختار سازمانی مورد نیاز خود را مد نظر قرار دهید.برخی شرکتها یا سازمانها یک ساختار متمرکز دارندنوعا

اینگونه سازمانها و شرکتها حوزه های اطلاعاتی قوی و محکمی دارندکه آنها را در یک ساختار شبکه ای با جزئیات کمتری تعریف و پیاده سازی می کنندامّا برخی دیگر از سازمانها و شرکتها بخصوص سازمانها و شرکتهای خیلی بزرگ پراکنده و غیر متمرکزنداینگونه سازمانها و شرکتها دارای شعبات چند گانه ای هستندکه هر کدام از آنها خیلی مهم و کانونی اند.اینگونه سازمانها به یک راهبرد غیرمتمرکز نیازمندند تا شبکه ها و اعضای خودشان را مدیریت کنند ACTIVE DIRECTORY .انعطاف پذیری که دارد شما میتوانید بهترین ساختار شبکه را برای سازمان خود ایجاد کرده و آن را برحتی کنترل کنید.شما در اکتیو دایرکتوری یوزرهای موجود در شبکه را تعریف کرده و قوانینی روی انها اعمال میکنید و شبکه خود را مدیریت میکنید.سروری که DOMAINمورد نظر شمارا مدیریت میکند DOMAIN CONTROLLER نام دارد یعنی این سرور حاوی تمامی اطلاعات مدیریتی میباشد .

عملیات AUTHENTICATION و AUTHORIZATION که عملیات تایید هویت کاربر بعد از زدن رمز عبور و یوزرنیم انجام میشود توسط همین اکتیودایرکتوری صورت میگیرد به این معنا که هنگامیکه سیستم عامل کاربران بالا می آید آنها یوزر نیم و پسورد تعیین شده را وارد کرده و این اطلاعات به سمت سرور اکتیو دایرکتوری مربوط به دامین رفته و در صورت صحیح بودن اطلاعات کاربری اجازه ورود کاربر به سیستم عامل خود را خواهد.در اکتیودایرکتوری تمامی دسترسی هایی که به کاربران داده شده است توسط این سرویس اعمال میگردد و هنگام ورود کاربران اعمال میشود به عنوان مثال مدیر شبکه اجازه اجرای برنامه را به شما نداده . این قانون هنگام ورود شما به سیستم بعد از وارد کردن رمز عبور و تایید آن بر روی سیستم شما اعمال میشود.اکتیودایرکتوری دارای دو جز مهم در شبکه میباشد :

۱. DNS
۲. DHCP

این سرویس به تنظیمات شبکه ما سرعت ، دقت و نظم می بخشد و بستری را ایجاد می کند تا شبکه کامپیوتری خود را مدیریت کنیم و تمامیOBJECT ها که شامل حساب کاربران و پرینترها و فایل های به اشتراک گذاشته شده همگی در این سرویس قرار دارند و میتوانیم آنهارا براحتی کنترل کنیم.شبکه ی استاندارد مبتنی بر ACTIVE DIRECTORY شامل موارد زیر است :

۱. سرور قدرتمند و استاندارد به همراه سیستم عامل ویندوز سرور
۲. ایستگاه های کاری مناسب جهت کار در شبکه با داشتن ویندوزهای مبتنی برNT
۳. شبکه کامپیوتری استاندارد مبتنی بر اصول کابل کشی ساخت یافته
۴. پروتکل TCP/IP و همچنین File Sharing در کلیه کامپیوترهای شبکه باید فعال باشند
۵. سیستم فایل سرور و در صورت امکان سیستم فایل های ایستگاه های کاری از نوع NTFS باشد
۶. در یک شبکه استاندارد آدرس IP سرور معمولا ثابت و دستی انتخاب می شود و ایستگاه های کاری آدرس خود را بطور اتوماتیک از DHCP شبکه دریافت می کنند.

۷. DNSزیر ساخت اصلیActive Directory می باشد. این سرویس بطور مستقل و یا در طول نصب Active Directoryقابل نصب می باشد.

مشخصات یک ACTIVE DIRECTORY خوب

۱. Centralization : اطلاعات را متمرکز می کند ،یعنی برای دسترسی به یک سری اطلاعات نیاز به جست و جوی در مکان های مختلف نباشد.

۲. Scalability : وقتی امکانات شبکه زیاد میشود یا به عبارت دیگر AD بزرگ میشود باید بتواند با آن گسترش کنار بیاید و سرعت آن کاهش پیدا نکند همچنین مانند سابق پرسش ها را سریعا جواب دهد، مثلا یک چاپگر خاص کجا قرار دارد.

۳. Standardization : بر اساس استانداردهای موجود دنیا تدوین شده باشد.

۴. Extensible : پذیرای افزایش قابلیتها باشد.هر برنامه ای که به سیستم عامل اضافه میشود ،ممکن است بخواهد خودش به AD یک سری موضوعات و قابلیت ها اضافه و از آنها استفاده نماید در نتیجه AD باید پذیرای افزایش قابلیت ها باشد.

۵. Seperation Of Physical Network : باید ساختار فیزیکی شبکه را از ساختار منطقی آن جدا کند و این هدف اصلی طراحی شبکه است ،چون لازم نیست کاربر بداند امکانات فیزیکی شبکه در کجا قرار دارد تا از آنها استفاده نماید.

۶. Security : امنیت در ذخیره اطلاعات و همچنین دسترسی به اطلاعات باید در AD وجود داشته باشد.

مراحل نصبACTIVE DIRECTORY

روش اول

۱. به کنسول دستور ویندوز رفته و از دستور"dcpromo" استفاده کنید. ویزارد نصب باز خواهد شد به ترتیبی که از شما خواسته شده عمل کرده و آن را به پایان برسانید.

۲. اگرکلمه عبور در طول نصب استفاده کرده اید آن را به خاطر سپرده و یا در جایی حفظ کنید زیرا در صورتی که بخواهید Active Directory راUninstall کنید به آن نیاز خواهید داشت.

۳. پس از نصب، سیستم را باید Restart کنید. اولین بار مدت بالا آمدن سیستم کمی طولانی تر خواهد بود.

روش دوم

شما به جای اینکه از طریق دامین کنترلر و از منوی administrative Tools به این کنسول دسترسی داشته باشید، می توانید از طریق یک Member Server و استفاده از کنسول MMC یا Microsoft Management Console و اضافه کردن کنسول Active Directory Users and Computers براحتی از این ابزار در سرور های دیگر نیز استفاده کنید .

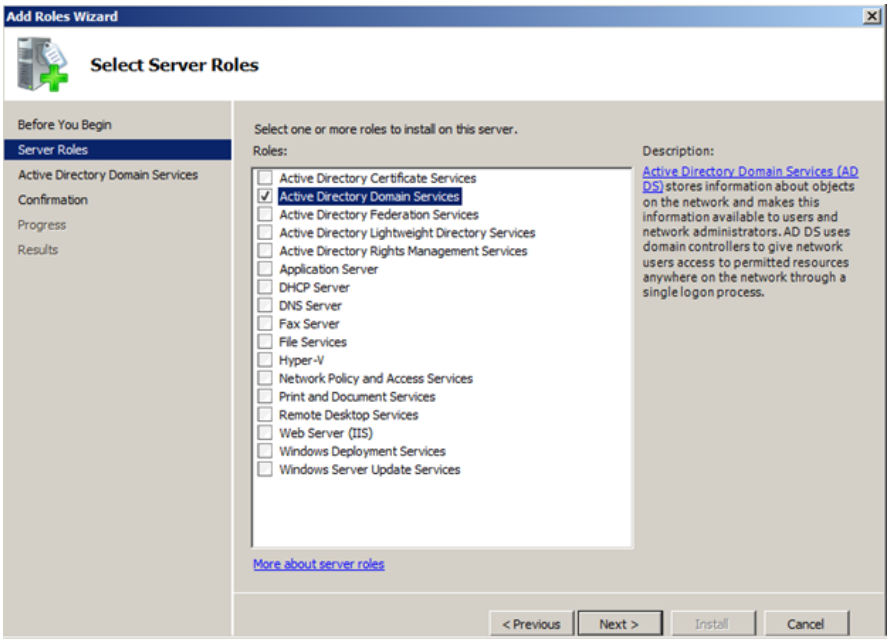
برای اینکار از طریق Run در منوی استارت دستور MMC را وارد کنید و کلید Enter را بزنید . در این لحظه سرور برای شما یک

صفحه کنسول خالی باز میکند . از طریق منوی File گزینه Add Remove Snap In را انتخاب کنید و از لیست موجود کنسول Active Directory Users and Computer را انتخاب کنید و بعد Close و OK را بزنید و منتظر باشید تا کنسول بصورت کامل لود شود .

روش اول تصویری

۱- Server Manager را باز کنید سپس به بخش Roles بروید و مسیر زیر را دنبال کنید:

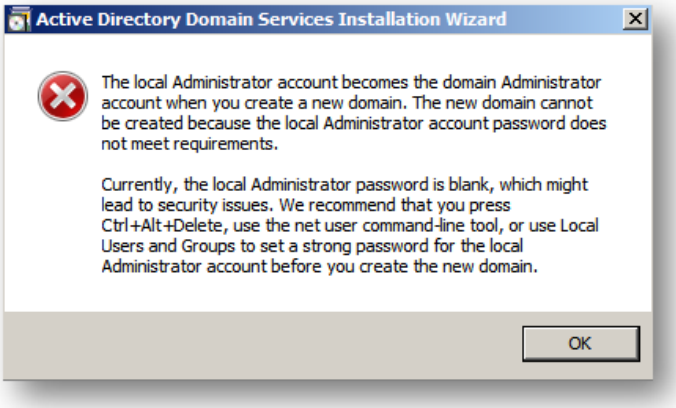
Add Roles → Active Directory Domain Services → Next → Install



Start → Run → dcpromo-2

پس از نصب به Start بروید و Run را باز کنید (کلید ترکیبی Win+R)و در آن dcpromo را نصب کنید.

Error Aministrator-3



Switch User → Administrator-4

با خطایی همچون بالا مواجه شدید باید فراموش نکنید که با یورز administrator به سیستم وارد شوید.

5- Active Directory Domain Services Installation Wizard →Next → Operating System Compatibility → Next

مراحل را همان گونه که می بینید طی کنید.

6- Choose a Deployment Configuration:

یکی از موارد زیر را انتخاب کنید:

Existing Forest

برای زمانی که می‌خواهیم یک دامین را در یک Forest عضو کنیم.

Create a New Domain in a New Forest:

برای زمانی که می‌خواهیم یک دامین جدید در یک forest جدید بسازیم.

7- Name the Forest Root Domain → Full Qualified Domain Name (FQDN) → Example: google.com

Set Forest Functional Level-8

Functional Levelدر یک تعریف ساده ویژگی‌ها و مُدهای عملیاتی Active Directory هستند که به هر نسخه از سیستم عامل ویندوز سرور اضافه می‌شوند و قابلیت‌هایی ویژه‌ای برای DC که تحت آن نسخه از سیستم عامل پیاده‌سازی شده است فراهم می‌کنند. شما هنگام نصب یک DC می‌توانید تعیین کنید که آن DC در سطح Domain و Forest طبق چه مُد از Functional Levelکار کند.

این موضوع از این لحاظ اهمیت دارد کهDC های زیادی در سطح Domain و Forest فعال هستند که باید دارای Functional Levelمناسب برای انجام صحیح وظایف و برقراری ارتباط با یکدیگر باشند Functional Level .در دو بخش طبقه‌بندی می‌شود:

الف :Domain Functional Level-ویژگی‌هایی از Active Directory که در یک Domain قابل دسترس هستند مشخص کرده و همچنین نسخه‌ای از ویندوز سرور را که می‌تواند به عنوان DC در Domain فعال باشد تعیین می‌کند.

ب :Forest Functional Level-ویژگی‌هایی از Active Directory که در یک Forest قابل دسترس هستند مشخص کرده و همچنین نسخه‌ای از ویندوز سرور را که می‌تواند به عنوان DC در Forest فعال باشد تعیین می‌کند.

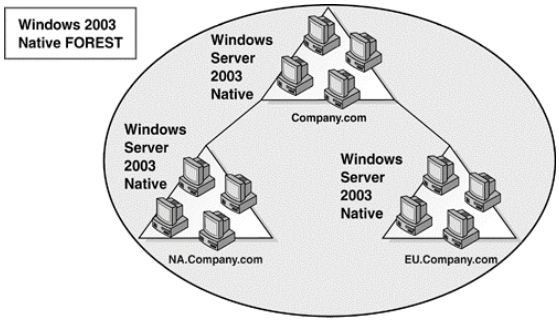
اما نسخه‌هایی از Functional Level تا Windows Server 2008 R2 عبارتند از:

- Windows 2000
- Windows 2003
- Windows 2008
- Windows 2008 R2

در هنگام نصب و راه‌اندازی Active Directory مرحله‌ای وجود دارد که شما می‌توانید Functional Level رو تعیین کنید . Forest Functional Levelرا تنها در زمان راه‌اندازی اولین DC یا به عبارتی Root Domain می‌توان تعیین کرد.

اما مفهوم کاربردی این مطالب چیست؟ فرض کنید شما در Windows Server 2008 R2 دامنه‌ای راه‌اندازی کرده و در هنگام تعیین Functional Level نسخه Windows۲۰۰۳ را برای Domain و Forest انتخاب کرده‌اید. در این حالت شما برای اضافه کردن هر DC دیگر به صورت Child و یا Additional می‌توانید کامپیوتری را که سیستم عامل آن نسخه Windows 2003به بعد است انتخاب کنید (یعنی Windows 2003, 2008 , 2008 R2, 2012) به فرض در این شرایط اگر بخواهید کامپیوتری با سیستم عامل Windows 2000 را به عنوان DC به این دامنه اضافه کنید با پیغام خطای Functional Level روبرو خواهید شد. حال فرض کنید اگر در ابتدا در هنگام تعیین Functional Level نسخه Windows 2008 R2 را انتخاب کرده باشید فقط می‌توانید از DC با سیستم عامل Windows 2008 R2 وWindows server 2012 را به دامنه خود اضافه کنید.

به یاد داشته باشید Functional Level را پس از انتخاب می‌توان به سمت نسخه بالاتر تغییر داد اما به سمت نسخه پایین خیر.



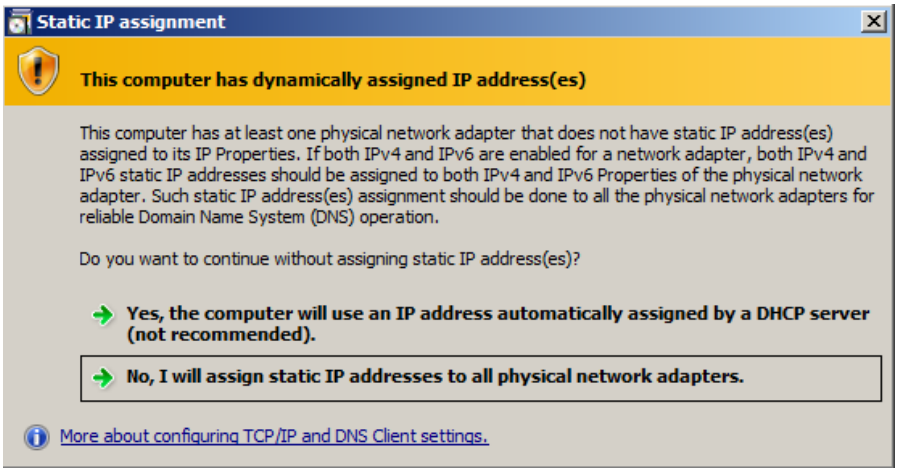
9-Additional Domain Controller Options → Gelobal Catalog:

اکتیو دایرکتوری امکان یافتن منابع همانند پرینترها، فایل‌ها و کاربران را فراهم می‌کند. یک سرویس کاتالوگ، شامل اطلاعات برگزیده‌ای از هر دامین در خصوص هر شیئیی است Global Catalog .سرویسی است که در اکتیو دایرکتوری برای یافتن منابع استفاده می‌شود.

Global Catalogیک انبار مرکزی اطلاعات است که اطلاعات گزینش شده‌ای در خصوص اشیاء موجود در یک جنگل، درخت یا دامین را شامل می‌شود. به صورت پیش فرض Global Catalog روی اولین دامین کنترلر در جنگل (Forest) جدید ساخته می‌شود. دامین کنترلری که این انبار اطلاعات روی آن قرار داشته باشد، Global Catalog Serverگفته می‌شود. در یک جنگل می‌توان هر دامین کنترلری را به عنوان Global Catalog Server تنظیم کرد.

از آنجایی که از مکانیسم Multi Master در Replication استفاده می‌شود، مشکلی در همسان سازی اطلاعات به وجود نخواهد آمد. به صورت پیش فرض این اطلاعات گزینش شده، اطلاعاتی است که بیشتر مورد جستجو قرار می‌گیرد. همانند نام و نام خانوادگی کاربران. این صفات در Active Directory Schema معین می‌شوند. همان‌طور که گفته شد، یکی از وظایف Global Catalogفراهم آوردن امکان جستجو و یافتن اطلاعات است. از آنجایی که اطلاعات سراسر یک جنگل در دسترس است، بدون توجه به آنکه شیئی در چه دامینی است می‌توان به جستجو پرداخت.

Error ip-10



11- Location For Database. Log File. Sysvol

12-Directory Services Restore Mode Aministrator Password:

پسوردی که در این قسمت وارد می‌شود بسیار مهم است و در Recovery کردن Backup اکتیو دایرکتوری و در هنگام پاک کردن اکتیو دایرکتوری لازم است

13-Next → Install

14- Restart

اگر مراحل را از بالا به پایین به صورت پشت سر هم طی کرده باشید و در پایان ری استارت انجام شده باشد اکتیو دایرکتوری شما نصب شده است.

وب سرور چیست؟

امروزه اطلاعات، در دنیای ما نقش بسیار مهمی دارند و بسیاری از این اطلاعات توسط اینترنت انتقال پیدا می‌کنند. متداولترین پروتکلی که برای انتقال اطلاعات از آن استفاده می شود، پروتکل HTTP است. پروتکل HTTP به عنوان پروتکلی سریع، قوی و با بار کم بر روی CPU و حافظه سرور طراحی شده است و البته برای جلوگیری از کاهش پیدا کردن کارایی وب بر اثر استفاده بسیار زیاد از این پروتکل، باید کارایی اش را بهینه سازی کرد.

دو استراتژی اصلی برای بهینه سازی کارایی وجود دارد:

۱- بهینه سازی کارایی وب سرور

۲- بهینه سازی کارایی پروتکل HTTP

البته یکی از چیزهایی که باعث می‌شود افراد سردرگم شوند حالت طراحی وب و مفهوم وب سرور است. بیشتر مردم فکر می‌کنند سرور یک ماشین فیزیکی بزرگ مثل سیستم کامپیوتری است که در یک اتاق سرد نگهداری می‌شود و یا حتی مثل سیستم هکرهاست! که همه فکر می‌کنند زیرِ زمین هستند.
از اینا گذشته واقعاً وب سرور چیست؟ حقیقت این است که سرور یک معنای نرم‌افزاری است و به معنای واقعی کلمه، یک سرویس است که بر روی یک رایانه اجرا می‌شود و نوع خدمتی که به مشتریان می‌دهد متفاوت و متعدد است. برای این عمل نیاز به یک سرور بزرگ و یا حتی یک پی سی نیست و حتی می‌توان این نرم‌افزار را با USB که روی آن نرم‌افزار XAMPP و ... نصب شده باشد، استفاده کرد.

البته وب سرور نرم‌افزار هایی مثل آپاچی روی یک سیستم کامپیوتری اختصاص داده شده است که می‌توانید از ویژگی‌های میزبانی وب اکثر سیستم عامل‌های ساخته شده مثل IIS ویندوز استفاده کنید و ضمناً خوب است بدانید اوبونتو هم یک وب سرور محسوب می شود.

در حقیقت راه اندازی یک وب سرور باعث می‌شود صفحات وبی که از کامپیوتر های دیگر ارایه شده، آسانتر و سریعتر باز شوند. البته وب سرور جنبه های پیچیده‌تری هم دارد، مثل ارائه محتوای پویا (داینامیک) با اشکال یا محتوای صفحاتی که اطلاعات ورودی کاربر را می پذیرد، پردازش آن‌ها، و حتی ایجاد صفحات سفارشی جدید.

وب سایت های سطح بالاتر شما را قادر می سازند با استفاده از نرم افزار هایی مانند آپاچی، که توانایی پردازش ورودی اطلاعات کاربران را دارد، به طور خودکار صفحات وب را ایجاد کنید و با استفاده از زبان های برنامه نویسی وب مانند PHP، جاوا و ... آن ها را کامل تر سازید.

ابتدا اجازه بدهید تنظیمات اولیه یک وب سرور را به شما ارائه بدهیم و شما آن را خوب بفهمید، سپس می توانید توضیحات بیشتری از آنچه یک وب سرور هست، به دست آورید.

وب سرور چیست و چگونه کار می کند؟

برای درک ساختار اصلی یک وب سرور، در مرحله اول نیاز است شما مسیر تبادل اطلاعات بین یک مرورگر وب از راه دور و یک وب سرور را درک کنید.

اولین راه ارتباطی، زمانی شروع می‌شود که یک نفر بر روی مرورگرش صفحه‌ای به عنوان وب سایت را باز کرده و در اینترنت جستجو می‌کند. حال همه اطلاعاتی که بر روی وب سرور ذخیره شده است که با درخواست کاربر اطلاعات برایش به نمایش گذاشته می‌شود.

در مورد ساختار مرورگرها در قالب تنها یک مطلب نمی‌شود توضیح داد پس بهتر است مقالات دیگر را برای آشنایی بیشتر با مرورگر مطالعه کنید.

به طور خلاصه اینکه مرورگرها با استفاده از DNS های دامنه که آن را به عنوان یک آدرس IP منحصر به فرد برای خر سایت می‌شناسند، می‌توانند به وسیله آن به سرورهای خاص دسترسی داشته باشند.

مرورگر پس از ایجاد ارتباط با سرویس دهنده های وب از طریق آدرس IP به درخواست صفحه مربوط به وب پاسخ می‌دهد. اساس صفحات وب، HTM یا فایل HTML است. صفحات پیش فرض به طور معمول برای بسیاری از وب سایت دارای فورمت های index.htm است و این همان فرضی است که اکثر وب سرورها بر آن استوارند و وقتی که درون مرورگر آدرس یک دامنه را وارد می‌کنید وب سرور به طور اتوماتیک فایل index.htm را که در معمولا دایرکتوری های اصلی اول وب سرور ها ذخیره می‌شود را برای شما ارسال می‌کند.

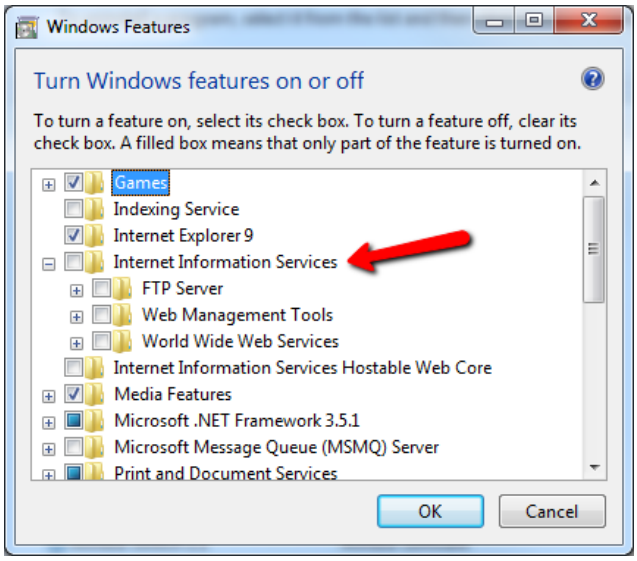
بعد از آن مرورگر شما می‌داند که کدهای HTML را چطور تفسیر کند و صفحه را به درستی به شما نمایش بدهد.

این مطلبی که گفته شد یک مسیر ساده است که بین وب سرور و کامپیوتر کاربر ایجاد می‌شود می‌توانید در عکس زیر مشاهده کنید.

واضح است که اینترنت کاملاً ساده هم نیست. (یعنی دقیقا چیزی که خیلی از ما ها به آن فکر می کنیم مثل روشن کردن مودم و .... نیست)

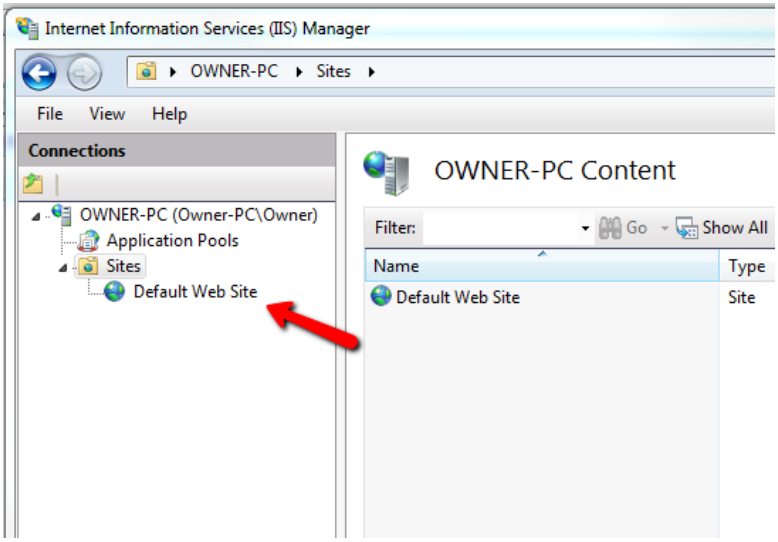
سایت‌های اینترنتی زیادی در جهان طراحی شده که فقط با راه اندازی تنها یک وب سرور می‌توان از هر نقطه دنیا به آن‌ها دسترسی داشت و در ظاهر نیاز به یک قلب (جایی برای متمرکز شدن) دارند .

راه اندازی یک وب سرور ساده برای در دسترس بودن فایل‌های HTML خیلی آسان است. اگر شما بخواهید یک وب سرور بر روی ویندوز ۷ راه اندازی کنید ابتدا باید از کنترل پنل "*Programs and Features*" را باز کنید و بعد روی دکمه " *Turn Windows features on or off*" کلیک کنید و در مرحله بعدی در قسمت "*Internet Information Services*" روی چک باکس آن کلیک کرده و آن را فعال کنید IIS وب سرور ویندوز است.



به طور پیش فرض، IIS یک سرور در FTP فعال نیست پس باید برروی چک باکس FTP server کلیک کنید و اگر هم بخواهید به فایل‌های کامپیوتر خود از راه دور دسترسی داشته باشید باید Web Management Tools را هم کلیک کنید.

در هر صورت، حال که وب سرور ویندوز یا IIS ای که بر روی کامپیوتر شما فعال شده است، هر فایل HTML امکان ذخیره شدن درمسیر دایرکتوری "C: \ inetpub \ wwwroot" را دارا خواهد بود و به کامپیوترهای دیگر نیز می توانید امکان دسترسی بدهید و این کار با رفتن به قسمت *Admin Tools و انتخاب گزینه "Internet Information Service" امکان‌پذیر است.*



این به این معنی است که اگر کامپیوتر شما به اینترنت هم وصل نباشد و در یک شرکت می‌توانید شبکه داخلی راه اندازی کنید و کامپیوترهای دیگر متصل به این شبکه، با وارد کردن IP یا نام رایانه می‌توانند به صفحات وب ذخیره شده برروی رایانه شما دسترسی داشته باشند.

این روش راه اندازی یک وب سرور ساده است.

اجرای برنامه‌ها و اسکریپت‌ها

درست است که این یک وب سرور ساده است اما اگه دوست داشته باشید کارهای جالبی می‌توانید بر روی آن انجام بدهید. مثلاً می‌خواهید کاربرها یک فرم را پر کنند و این اطلاعات در یک جایی ذخیره بشوند یا اینکه یک وبلاگ روی هاست وردپرس داشته باشید، امکان دارد؟ بله شما باید سرور برنامه نویسی را هم فعال کنید.

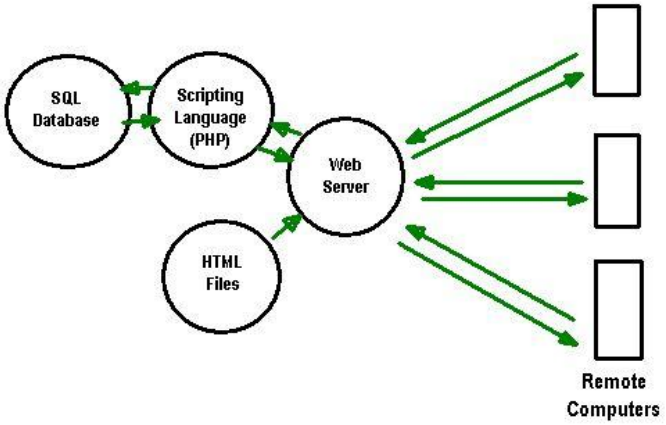
وب سرور برای برطرف کردن نیاز کاربرانش یک سری موارد را روی خودش نصب کرده است زبان هایی مانند: روبی، جاوا، PHP، سی پلاس پلاس، دات نت، و بسیاری موارد دیگر. و نکته تعجب آورش این است که شما باید بدانید برای نوشتن برنامه‌های کاربردی چه زبانی را انتخاب کنید، که این برنامه کاربری باید بر روی مرورگر هم اجرا شود.

برای اینکه شما در وقتتان صرفه جویی کنید می‌توانید به راهنمای راه اندازی XAMPP (یک برنامه برای ساخت وب سرور داخلی یا لوکال) بر روی کامپیوتر تان مراجعه کنید.

البته این فقط یک پیشنهاد است و این در حالی است که برنامه دیگری هم وجود دارد.

اساساً کار یک وب سرور مثل آپاچی (یا هر نوع وب سرور دیگری که میزبان اطلاعات موجود بر روی کامپیوتر شماست)، زبان برنامه نویسی PHP، زبان برنامه نویسی پرل، و پایگاه داده MySQL است.

اگر وب سرور به طور دقیق نصب شده باشد کارکرد سیستم تان شبیه به عکس زیر می‌شود.



در حال حاضر شما با وب سرورتان از راه دور (یا لوکال) به کامپیوترتان دسترسی دارید و می‌توانید فایل‌های استاتیک و پویای خود را دریافت کنید و اگر در یک وبلاگ وردپرس یک سری صفحات ایجاد کنید، می‌توانید به راحتی آن‌ها را ببینید و از راه دور لود کنید. وب سرور، خروجی منحصر به فردی دارد که شامل خروجی اسکریپت و ... می شود که در صورت لزوم امکان دسترسی به پایگاه داده‌ای (SQL) که بر روی وب سرور ذخیره شده است را هم می‌توان داد.

همانطور که می بینید، شما می‌توانید به وب سرور، زبان‌های برنامه نویسی مختلف را اضافه کنید و در پایگاه داده اطلاعات زیادی را ذخیره کنید با این وضعیت شما می‌توانید یک وب سایت با امکانات نامحدود داشته باشید. حتی می‌توانید از تمام فایل‌ها و پوشه‌های مربوط به وب سایتتان بک آپ بگیرید و یا حتی آن‌ها را با همین تنظیمات به وب سرور دیگری منتقل کنید.

با USB شما فقط می‌توانید هر بار فقط با یک کامپیوتر ارتباط داشته باشید، به همین دلیل میزبانی وب سرور با یو اس بی و XAMPP خیلی مورد استقبال قرار نگرفته است.
همانطور که متوجه شدید در وب سرور بیشتر بحث نرم افزاری است تا کامپیوتر واقعی، و درواقع این نرم افزارها هستند که به شما این امکان را می‌دهد که تمام فایل‌های وب جهان را باز کنید.