دانشگاه صنعتی اصفهان

جمهوری اسلامی ایران
وزارت علوم تحقیقات و فناوری

دانشگاه جامع
علمی-کاربردی

Computer Networks Workshop

آزمایشگاه شبکه های کامپیوتری

آنچه در این مجموعه آموزشی می خوانید :

- ✓ مفاهیم شبکه های کامپیوتری
- ✓ توپولوژی های شبکه
- ✓ انوع تجهیزات شبکه
- ✓ شبکه های PtP و SB
- ✓ راه اندازی شبکه Work Group
- ✓ ویندوز Server 2003
- ✓ مفاهیم Domain و راه اندازی آن
- ✓ Group Policy
- ✓ نقش ها و سرویس های ویندوز Server
- ✓ و ...

ویرایش دوم

رضا رمضانی

R.Ramezani@ec.iut.ac.ir

پاییز ۱۳۹۰

آزمایشگاه شبکه های کامپیوتری

قابل استفاده دانشجویان

رشته فناوری اطلاعات و ارتباطات و نرم افزار کامپیوتر

«من ستایشگر معلمی هستم که اندیشیدن را به من بیاموزد، نه اندیشه ها را»

شهید مرتضی مطهری

مدرس : رضا رمضانی

تقدیم به ساحت مقدس

حضرت فاطمه زهرا (س) و یوسف گمشده اش

و پیشکش آنان که دل هایشان به وسعت دریاست

و اندیشه هایشان از آن هم وسیع تر...

آنان که به رسم ادب این اوراق را تورق می کنند

گرچه از آن مستغنی اند.

پیشگفتار

خداوند منان را شاکرم که در این ترم تحصیلی، مجددا توفیق خدمت در زمینه علم و دانش را به بنده عطا فرمود و توانستم در این زمینه گام کوچکی بردارم. همانطوری که می دانید یکی از مهمترین دروس دانشجویان رشته کامپیوتر، به خصوص دانشجویان رشته *فناوری اطلاعات و ارتباطات*، درس *آزمایشگاه شبکه های کامپیوتری* می باشد. زیرا امروزه اکثر شرکت های تجاری، نیاز زیادی به شبکه سازی رایانه ها و دفاتر تجاری خود دارند و وجود یک متخصص شبکه و IT در هر شرکتی ضروری به نظر می رسد. اما متاسفانه در مراکز آموزش عالی، به این درس توجه زیادی نمی شود. یکی دیگر از مشکلات این درس، کمبود منابع درسی *جامع و کامل*، به طوری که بتواند مباحث عملی شبکه را به خوبی پوشش دهد می باشد. لذا بنده بر خود لازم دانستم که مطالب مرتبط با این درس را جمع آوری نموده و در قالب یک جزوه آموزشی قرار دهم تا هم کمبودهای آموزشی دانشجویان مرتفع گردد و هم اگر دانشجویی قصد داشت در آینده مباحث شبکه را ادامه دهد، منبعی برای آغاز کار خود داشته باشد. لذا در تهیه این جزوه هم مباحث ابتدایی و هم مباحث متوسط و پیشرفته درس *آزمایشگاه شبکه های کامپیوتری* قرار گرفته است. برخی از فصول این جزوه، فقط به مباحث تئوری شبکه های کامپیوتری می پردازد. فصل هایی هم که مباحث عملی را توضیح می دهند در دو قسمت سازماندهی شده اند، بخش اول آن ها، آموزش تئوری و مفاهیم پایه ای در مورد مباحث آن فصل است و بخش دوم نیز به آموزش عملی آن مبحث می پردازد که در تمام فصول عملی، سعی بر آن شده است که به همراه آموزش عملی، تصاویری را نیز قرار دهم تا درک مطالب راحت تر شود. لازم به ذکر است که در برخی از فصول این جزوه از تحقیقات ارائه شده دانشجویان استفاده شده است.

به دانشجویان و مدرسین عزیز توصیه می کنم که مطالب این جزوه را حتما با کمک نرم افزار شبیه سازی Oracle VM Virtual Box به صورت عملی کار کنند. آموزش این نرم افزار در همین جزوه قرار داده شده است.

این جزوه آموزشی نیز مانند بسیاری از منابع آموزشی، عاری از خطا و اشتباه نیست و مسلما خطاها و اشتباهات زیادی چه از نظر فنی و چه از نظر محتوایی در بین مطالب وجود دارد؛ لذا از تمامی دانشجویان خواهشمندم که مشکلات این جزوه را به من اطلاع دهند تا آنها را تصحیح کنم تا بتوانیم جزوه ای کم نقص را با کمک یکدیگر آماده سازیم. امید است که این مجموعه آموزشی مورد قبول و رضایت خداوند متعال و شما دانشجویان گرامی قرار گیرد.

رضا رمضانی

Weblog : http://Ramezani-cs.blogfa.com

Email : R.Ramezani@ec.iut.ac.ir

ای خدا! من باید از نظر علم نیز از همه برتر باشم تا مبادا که دشمنان، مرا از این راه طعنه زنند. باید به آن سنگ دلانی که علم را بهانه کرده و به دیگران فخر می فروشند، ثابت کنم که خاک پای من هم نخواهند شد. باید همه آن تیره دلان مغرور و متکبر را به زانو در آورم؛ آنگاه خود خاضع ترین و افتاده ترین فرد روی زمین باشم.

از نیایش های دکتر چمران - سپتامبر ۱۹۶۱ – دانشگاه بِرکلی آمریکا

فهرست مطالب (۱)

فهرست مطالب (۲)

فهرست مطالب (۳)

فهرست مطالب (۴)

فهرست مطالب (۵)

فهرست مطالب (۶)

فهرست مطالب (۷)

فهرست مطالب (۸)

فهرست مطالب (۹)

فهرست مطالب (۱۰)

فهرست مطالب (۱۱)

فهرست مطالب (۱۲)

فهرست مطالب (۱۳)

فصل ۱

آشنایی با شبکه

۱-۱- معرفی

یک شبکه رایانه ای، اجازه به اشتراک گذاری منابع و اطلاعات در میان دستگاه ها و سیستم های متصل شده به هم را می دهد. در دهه ۶۰ میلادی، آژانس پروژه های تحقیقاتی پیشرفته (ARPA)، بودجه ای را به منظور طراحی شبکه آژانس پروژه های تحقیقاتی پیشرفته (ARPANET) برای وزارت دفاع ایالات متحده آمریکا اختصاص داد. این اولین شبکه رایانه ای در جهان بود. توسعه شبکه از سال ۱۹۶۹ و براساس طرح های توسعه یافته دهه ۶۰ آغاز شد.

۱-۲- تاریخچه شبکه

در سال ۱۹۵۷ نخستین ماهواره، یعنی اسپوتنیک توسط اتحاد جماهیر شوروی سابق به فضا پرتاب شد. در همین دوران دنیا در دوران رقابت سختی از نظر تسلیحاتی بین دو ابر قدرت آن زمان جریان داشت و دنیا در دوران جنگ سرد به سر می برد. وزارت دفاع امریکا در واکنش به این اقدام رقیب نظامی خود، آژانس پروژه های تحقیقاتی پیشرفته یا آرپا (ARPA) را تاسیس کرد. یکی از پروژه های مهم این آژانس تامین ارتباطات در زمان جنگ جهانی احتمالی تعریف شده بود. در همین سال ها در مراکز تحقیقاتی غیر نظامی که بر امتداد دانشگاه ها بودند، تلاش برای اتصال کامپیوتر ها به یکدیگر در جریان بود. در آن زمان کامپیوتر های Mainframe از طریق ترمینال ها به کاربران سرویس می دادند. در اثر اهمیت یافتن این موضوع آژانس آرپا (ARPA) منابع مالی پروژه اتصال دو کامپیوتر از راه دور به یکدیگر را در دانشگاه MIT بر عهده گرفت. در اواخر سال ۱۹۶۰ اولین شبکه کامپیوتری بین چهار کامپیوتر که دو تای آنها در MIT، یکی در دانشگاه کالیفرنیا و دیگری در مرکز تحقیقاتی استنفورد قرار داشتند، راه اندازی شد. این شبکه آرپانت نامگذاری شد. در سال ۱۹۶۵ نخستین ارتباط راه دور بین دانشگاه MIT و یک مرکز دیگر نیز برقرار گردید. در سال ۱۹۷۰ شرکت معتبر زیراکس یک مرکز تحقیقاتی در پالوآلتو تاسیس کرد. این مرکز در طول سال ها مهمترین فناوری های مرتبط با کامپیوتر را معرفی کرده است و از این نظریه به یک مرکز تحقیقاتی افسانه ای بدل گشته است. این مرکز تحقیقاتی که پارک (PARC) نیز نامیده می شود، به تحقیقات در زمینه شبکه های کامپیوتری پیوست. تا این سال ها شبکه آرپانت به امور نظامی اختصاص داشت، اما در سال ۱۹۷۲ به عموم معرفی شد. در این سال شبکه آرپانت مراکز کامپیوتری بسیاری از دانشگاه ها و مراکز تحقیقاتی را به هم متصل کرده بود. در سال ۱۹۷۲ نخستین نامه الکترونیکی از طریق شبکه منتقل گردید. در این سال ها حرکتی غیر انتفاعی به نام MERIT که چندین دانشگاه بنیان گذار آن بوده اند، مشغول توسعه روش های اتصال کاربران ترمینال ها به کامپیوتر مرکزی یا میزبان بود. مهندسان پروژه MERIT در تلاش برای ایجاد ارتباط بین کامپیوتر ها، مجبور شدند تجهیزات لازم را خود طراحی کنند. آنان با طراحی

تجهیزات واسطه برای مینی کامپیوتر DECPDP-11 نخستین بستر اصلی یا Backbone شبکه کامپیوتری را ساختند. تا سال ها نمونه های اصلاح شده این کامپیوتر با نام PCP یا Processor Communications Primary نقش میزبان را در شبکه ها ایفا می کرد. نخستین شبکه از این نوع که چندین ایالت را به هم متصل می کرد Michnet نام داشت. روش اتصال کاربران به کامپیوتر میزبان در آن زمان به این صورت بود که یک نرم افزار خاص بر روی کامپیوتر مرکزی اجرا می شد. و ارتباط کاربران را برقرار می کرد. اما در سال ۱۹۷۶ نرم افزار جدیدی به نام Hermes عرضه شد که برای نخستین بار به کاربران اجازه می داد تا از طریق یک ترمینال به صورت تعاملی مستقیماً به سیستم MERIT متصل شوند. این، نخستین باری بود که کاربران می توانستند در هنگام برقراری ارتباط از خود بپرسند: کدام میزبان؟ از وقایع مهم تاریخچه شبکه های کامپیوتری، ابداع روش سوئیچینگ بسته ای یا Packet Switching است. قبل از معرفی شدن این روش از سوئیچینگ مداری یا Circuit Switching برای تعیین مسیر ارتباطی استفاده می شد. اما در سال ۱۹۷۴ با پیدایش پروتکل ارتباطی TCP/IP از مفهوم Packet Switching استفاده گسترده تری شد. این پروتکل در سال ۱۹۸۲ جایگزین پروتکل NCP شد و به پروتکل استاندارد برای آرپانت تبدیل گشت. در همین زمان یک شاخه فرعی بنام MILnet در آرپانت همچنان از پروتکل قبلی پشتیبانی می کرد و به ارائه خدمات نظامی می پرداخت. با این تغییر و تحول، شبکه های زیادی به بخش تحقیقاتی این شبکه متصل شدند و آرپانت به اینترنت تبدیل گشت. در این سال ها حجم ارتباطات شبکه ای افزایش یافت و مفهوم ترافیک شبکه مطرح شد. مسیر یابی در این شبکه به کمک آدرس های IP به صورت ۳۲ بیتی انجام می گرفته است. هشت بیت اول آدرس IP به شبکه های محلی تخصیص داده شده بود که به سرعت مشخص گشت تناسبی با نرخ رشد شبکه ها ندارد و باید در آن تجدید نظر شود. مفهوم شبکه های LAN و شبکه های WAN در سال دهه ۷۰ میلادی از یکدیگر تفکیک شدند. در آدرس دهی ۳۲ بیتی اولیه، بقیه ۲۴ بیت آدرس به میزبان در شبکه اشاره می کرد. در سال ۱۹۸۳ سیستم نامگذاری دامنه ها (Domain Name System) به وجود آمد و اولین سرویس دهنده نامگذاری(Name Server) راه اندازی شد و استفاده از نام به جای آدرس های عددی معرفی شد. در این سال تعداد میزبان های اینترنت از مرز ده هزار عدد فراتر رفته بود.

۱-۳- تعریف شبکه

شبکه های کامپیوتری، مجموعه ای از کامپیوتر های **مستقل و متصل** به یکدیگرند که با یکدیگر ارتباط داشته و تبادل اطلاعات می کنند. مستقل بودن کامپیوتر ها بدین معناست که هر کدام دارای واحدهای کنترلی و پردازشی مجزا بوده و بود و نبود یکی بر دیگری تاثیرگذار نیست.

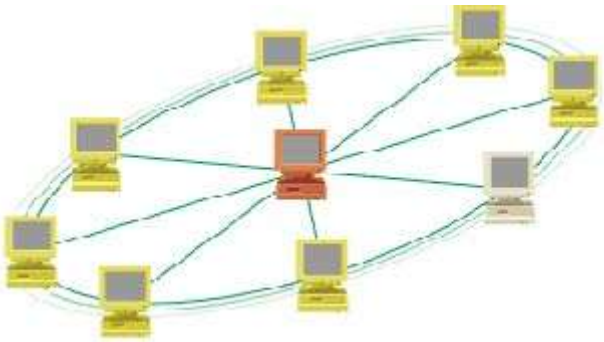
متصل بودن کامپیوتر ها یعنی کامپیوتر ها از طریق یک رسانه مانند کابل، فیبر نوری، ماهواره ها و... به هم متصل می باشند. دو شرط فوق، شروط لازم برای ایجاد یک شبکه کامپیوتری می باشد؛ اما شرط کافی برای تشکیل یک شبکه کامپیوتری داشتن ارتباط و تبادل داده بین کامپیوتر ها است.

این موضوع در بین متخصصین قلمرو شبکه مورد بحث است که آیا دو رایانه که با استفاده از نوعی از رسانه ارتباطی به یکدیگر متصل شده اند، تشکیل یک شبکه می دهند یا خیر. در این باره بعضی مطالعات می گویند که یک شبکه نیازمند دست کم ۳ رایانه متصل به هم است. یکی از این منابع با عنوان ارتباطات راه دور: واژه نامه اصطلاحات ارتباطات راه دور، یک شبکه رایانه ای را این طور تعریف می کند: شبکه ای از گره های پردازشگر Data که جهت ارتباطات Data به یکدیگر متصل شده اند. در همین سند عبارت شبکه این طور تعریف شده است: اتصال سه یا چند نهاد ارتباطی. رایانه ای که به دستگاهی غیر رایانه ای متصل شده است (به عنوان نمونه از طریق ارتباط اترنت به یک چاپگر متصل شده است) ممکن است که یک شبکه رایانه ای به حساب آید، اگرچه این نوشتار به این نوع پیکربندی نمی پردازد.

این نوشتار از تعاریفی استفاده می کند که به دو یا چند رایانه متصل به هم نیازمند است تا تشکیل یک شبکه را بدهد. در مورد تعداد بیشتری رایانه که به هم متصل هستند، عموماً توابع پایه ای مشترکی دیده می شود. از این بابت برای آنکه شبکه

ای به وظیفه اش عمل کند، سه نیاز اولیه بایستی فراهم گردد، اتصالات، ارتباطات و خدمات. **اتصالات** به بستر سخت افزاری اشاره دارد، **ارتباطات** به روشی اشاره می کند که بواسطه آن وسایل با یکدیگر صحبت کنند و **خدمات** آنهایی هستند که برای بقیه اعضای شبکه به اشتراک گذاشته شده اند.

اما در یک تعریف کلی می توان گفت که شبکه مجموعه ای از کامپیوتر ها، نرم افزار و سخت افزارهای متصل به هم است که باعث می شود کاربران بتوانند با یکدیگر کار کنند.



۱-۴- هدف از ایجاد شبکه چیست؟

به طور کلی اهدافی مثل زیر در ایجاد یک شبکه کامپیوتری دنبال می شود:

۱. استفاده مشترک از منابع
۲. استفاده از منابع راه دور
۳. افزایش امنیت و انعطاف پذیری
۴. مکانیزه کردن یا اتوماسیون کردن مجموعه ها
۵. استفاده بهینه از وقت و امکانات و صرفه جویی در هزینه ها

به نظر می رسد که همین موارد دلایل خوبی برای به راه انداختن یک شبکه می باشد. ضمن اینکه موارد متعدد دیگری نیز موجود می باشد.

۱-۵- مزایای شبکه

۱. استفاده از منابع مشترک (اطلاعات، نرم افزارها و سخت افزارها)
۲. حذف محدودیتهای جغرافیایی
۳. تبادل سریع تر و دقیق تر اطلاعات
۴. صرفه جویی در هزینه ها
۵. افزایش امنیت

اما در مطالب فوق یک کلمه به نام منابع را بکار بردیم آیا می دانید منابع چه هستند؟

منظور از منابع در کامپیوتر ها امکانات آنها مثل پردازنده مرکزی، هارد دیسک، چاپگر که جزء منابع سخت افزاری هستند و بانکهای اطلاعاتی، فایلهای صوتی و تصویری به عنوان منابع نرم افزاری می باشد.

۱-۶- دسته بندی شبکه های رایانه ای

در بحث شبکه های کامپیوتری دسته بندی های مختلفی وجود دارد که به مرور آنها را بررسی خواهیم نمود.

۱-۶-۱- بر اساس نوع اتصال

شبکه های رایانه ای را می توان با توجه به تکنولوژی سخت افزاری و یا نرم افزاری که برای اتصال دستگاه های شبکه استفاده می شود، دسته بندی کرد؛ مانند **فیبر نوری، اترنت، شبکه بی سیم، ارتباط خط نیرو یا G.hn**.

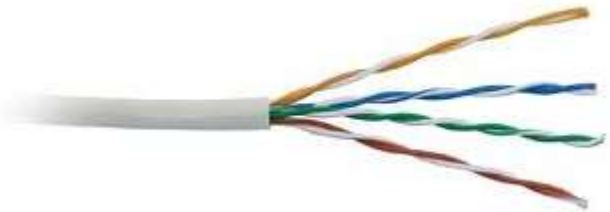
اترنت با استفاده از سیم کشی فیزیکی دستگاه ها را به هم متصل می کند. دستگاه های مستقر معمول شامل هاب ها، سوئیچ ها، پل ها و یا مسیریاب ها هستند.

تکنولوژی **شبکه بی سیم** برای اتصال دستگاه ها، بدون استفاده از سیم کشی طراحی شده است. این دستگاه ها از امواج رادیویی یا سیگنالهای مادون قرمز به عنوان رسانه انتقال استفاده می کنند.

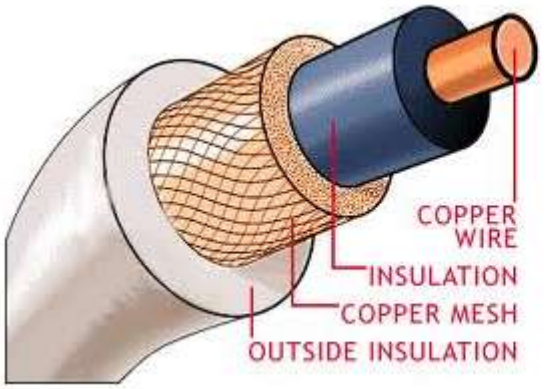
فناوری ITU-T G.hn از سیم کشی موجود در منازل (کابل هم محور، خطوط تلفن و خطوط برق) برای ایجاد یک شبکه محلی پر سرعت (تا۱ گیگابیت در ثانیه) استفاده می کند.

۱-۶-۲- بر اساس تکنولوژی سیم کشی

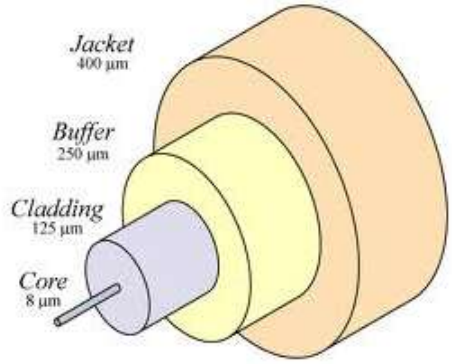
۱- زوج به هم تابیده (Twisted Pair): زوج به هم تابیده یکی از بهترین رسانه های مورد استفاده برای ارتباطات راه دور می باشد. سیم های زوج به هم تابیده، سیم تلفن معمولی هستند که از دو سیم مسی عایق که دو به دو به هم پیچ خورده اند درست شده اند. از زوج به هم تابیده برای انتقال صدا و داده ها استفاده می شود. استفاده از دو سیم به هم تابیده به کاهش تداخل و القای الکترومغناطیسی کمک می کند. سرعت انتقال داده، دامنه ای از ۲ مگابیت در هر ثانیه تا ۱۰۰ مگابیت در هر ثانیه دارد.



۲- کابل هم محور (Coaxial): کابل هم محور به طور گسترده ای در سیستم های تلویزیون کابلی، ساختمان های اداری، و دیگر سایت های کاری برای شبکه های محلی، استفاده می شود. کابل ها یک رسانای داخلی دارند که توسط یک عایق منعطف محصور شده اند، که روی این لایه منعطف نیز توسط یک رسانای نازک برای انعطاف کابل، به هم بافته شده است. همه این اجزا، در داخل عایق دیگری جاسازی شده اند. لایه عایق به حداقل رساندن تداخل و اعوجاج کمک می کند. سرعت انتقال داده، دامنه ای از ۲۰۰ میلیون تا بیش از ۵۰۰ میلیون بیت در هر ثانیه دارد.



۳- فیبر نوری: کابل فیبر نوری شامل یک یا چند رشته از الیاف شیشه ای پیچیده شده در لایه های محافظ می باشد. این کابل می تواند نور را تا مسافت های طولانی انتقال دهد. کابل های فیبر نوری تحت تاثیر تابش های الکترومغناطیسی قرار نمی گیرند. سرعت انتقال ممکن است به چند تریلیون بیت در ثانیه برسد.



۱-۶-۳- بر اساس تکنولوژی بی سیم

۱- ریز موج (مایکروویو) زمینی: ریز موج های زمینی از گیرنده ها و فرستنده های زمینی استفاده می کنند. تجهیزات این تکنولوژی شبیه به دیش های ماهواره است. مایکروویو زمینی از دامنه های کوتاه گیگاهرتز استفاده می کند، که این سبب می شود تمام ارتباطات به صورت دید خطی محدود باشد. فاصله بین ایستگاههای رله (تقویت سیگنال) حدود ۳۰ مایل است. آنتن های ریز موج معمولاً در بالای ساختمان ها، برج ها، تپه ها و قله کوه نصب می شوند.

۲- ماهواره های ارتباطی: ماهواره ها از ریز موج های رادیویی که توسط جو زمین منحرف نمی شوند، به عنوان رسانه مخابراتی خود استفاده می کنند. ماهواره ها در فضا مستقر هستند؛ به طور معمول ۲۲۰۰۰ مایل (برای ماهواره های Geosynchronous) بالاتر از خط استوا. این سیستم های در حال چرخش به دور زمین، قادر به دریافت و رله صدا، داده ها و سیگنال های تلویزیونی هستند.

۳- تلفن همراه: سیستم های تلفن همراه از چندین فناوری ارتباطات رادیویی استفاده می کنند. این سیستم ها به مناطق مختلف جغرافیایی تقسیم شده اند. هر منطقه دارای فرستنده های کم قدرت و یا دستگاه های رله رادیویی آنتن برای تقویت تماس ها از یک منطقه به منطقه بعدی است.

۴- شبکه های محلی بی سیم: شبکه محلی بی سیم از یک تکنولوژی رادیویی فرکانس بالا (مشابه سلول دیجیتالی) و یک تکنولوژی رادیویی فرکانس پایین استفاده می کند. شبکه های محلی بی سیم از تکنولوژِی طیف گسترده، برای برقراری ارتباط میان دستگاه های متعدد در یک منطقه محدود، استفاده می کنند. نمونه ای از استاندارد تکنولوژی بی سیم، موج رادیویی IEEE است.

۵- ارتباطات مادون قرمز: ارتباط فروسرخ، سیگنال های بین دستگاه ها را در فواصل کوچک (کمتر از ۱۰ متر) به صورت همتا به همتا (رو در رو) انتقال می دهد؛ در خط انتقال نباید هیچ گونه شی ای قرار داشته باشد.

۱-۶-۴- بر اساس اندازه

ممکن است شبکه های رایانه ای بر اساس اندازه یا گستردگی ناحیه ای که شبکه پوشش می دهد طبقه بندی شوند. برای نمونه شبکه شخصی (PAN)، شبکه محلی (LAN)، شبکه دانشگاهی (CAN)، شبکه کلان شهری (MAN)، شبکه گسترده (WAN) و شبکه های متصل.

۱- شبکه شخصی (Personal Area Network): یک شبکه رایانه ای است که برای ارتباطات میان وسایل رایانه ای که اطراف یک فرد می باشند (مانند تلفن ها و رایانه های جیبی (PDA) که به آن دستیار دیجیتالی شخصی نیز می گویند) بکار می رود. این که این وسایل ممکن است متعلق به آن فرد باشند یا خیر جای بحث خود را دارد. برد یک شبکه شخصی عموماً چند متر بیشتر نیست. موارد مصرف شبکه های خصوصی می تواند جهت ارتباطات وسایل شخصی چند نفر به یکدیگر و یا برقراری اتصال این وسایل به شبکه ای در سطح بالاتر و شبکه اینترنت باشد.

ارتباطات شبکه های شخصی ممکن است به صورت سیمی به گذرگاه های رایانه مانند USB و FireWire برقرار شود. همچنین با بهره گیری از فناوری هایی مانند IrDA، بلوتوث و UWB می توان شبکه های شخصی را به صورت بیسیم ساخت.

۲- شبکه محلی (Local Area Network): یک شبکه رایانه ای است که محدوده جغرافیایی کوچکی مانند یک خانه، یک دفتر کار یا گروهی از ساختمان ها را پوشش می دهد. در مقایسه با شبکه های گسترده (WAN) از مشخصات تعریف شده شبکه های محلی می توان به موارد زیر اشاره کرد:

۱. سرعت (نرخ انتقال) بسیار بالاتر از Wan

۲. محدوده جغرافیایی کوچکتر و عدم نیاز به خطوط استیجاری مخابراتی

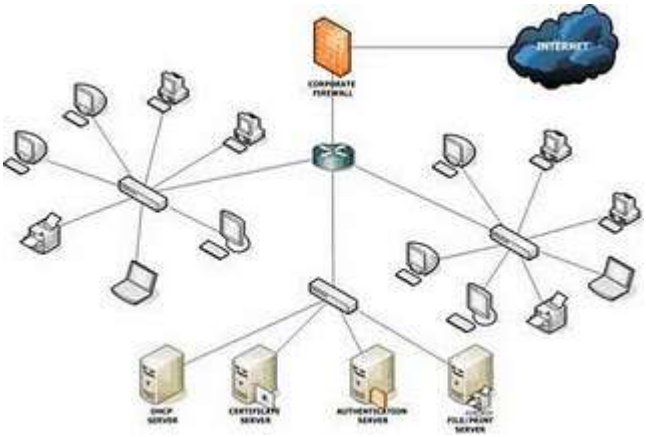
۳. امنیت بالاتر

۴. تعداد کامپیوتر کمتر

۵. مدیریت راحت تر

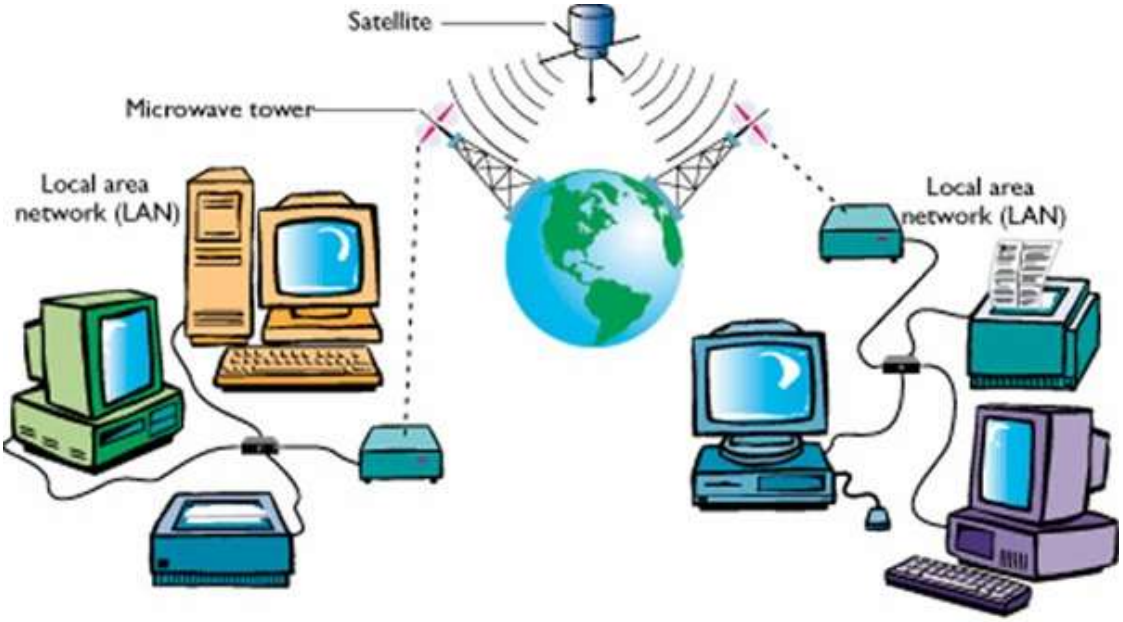
دو فناوری اترنت (Ethernet) روی کابل جفت به هم تابیده بدون محافظ (UTP) و وای فای (Wi-Fi) رایج ترین فناوری هایی هستند که امروزه استفاده می شوند، با این حال فناوری های آرکنِت (ARCNET) و توکن رینگ (Token Ring) و بسیاری روشهای دیگر در گذشته مورد استفاده بوده اند.

۳- شبکه دانشگاهی (Campus Area Network): که در بعضی ترجمه ها، به آن شبکه پردیس نیز گفته اند که یک شبکه رایانه ای است که از اتصال چند شبکه محلی (LAN) که همه آنها محدود به یک ناحیه جغرافیایی هستند ساخته می شود، مانند محوطه یک دانشگاه، یک مجموعه صنعتی یا یک پایگاه نظامی. می توان آن را به عنوان یکی از انواع شبکه های کلان شهری (MAN) به حساب آورد که عموماً محدود به ناحیه ای کوچک تر از اندازه معمول یک شبکه کلان شهری است. در حالتی که در فضای یک دانشگاه شبکه ای از نوع شبکه دانشگاهی داشته باشیم، شبکه مورد نظر محتملا ساختمان های دانشکده های مختلف شامل بخش های آکادمیک، کتابخانه دانشگاه و ساختمان محل اقامت دانشجویان را به یکدیگر متصل می کند. شبکه دانشگاهی بزرگ تر از یک شبکه محلی ولی کوچکتر از یک شبکه گسترده (WAN) است.



۴- شبکه کلان شهری (Metropolitan Area Network): یک شبکه رایانه ای بزرگ است که معمولاً در سطح یک شهر گسترده می شود. در این شبکه ها معمولاً از زیرساخت بیسیم و یا اتصالات فیبر نوری جهت ارتباط محل های مختلف استفاده می شود. به عبارت دیگر شبکه Man، به شبکه هایی ما بین شبکه های LAN و WAN گفته می شود و یک راه تشخیص آن، این است که از تجهیزات مخابراتی آنچنانی استفاده نمی شود. مثلاً اگر شرکتی در یک شهر دارای چند شعبه باشد و بخواهید آن شعبه ها را به یکدیگر متصل کند، یک چنین شبکه ای ایجاد می کند

۵- شبکه گسترده (Wide Area Network): یک شبکه رایانه ای است که نسبتاً ناحیه جغرافیایی وسیعی را پوشش می دهد (برای نمونه از یک کشور به کشوری دیگر یا از یک قاره به قاره ای دیگر). این شبکه ها معمولاً از امکانات انتقال خدمات دهندگان عمومی مانند شرکت های مخابرات استفاده می کند. به عبارت کمتر رسمی این شبکه ها از مسیریاب ها و لینک های ارتباطی عمومی استفاده می کنند.



۶- شبکه متصل (Internetwork): دو یا چند شبکه یا زیرشبکه (Subnet) که با استفاده از تجهیزاتی که در لایه ۳ یعنی لایه شبکه مدل مرجع OSI (این لایه را در فصل های بعدی معرفی خواهیم نمود) عمل می کنند؛ مانند یک مسیریاب، به یکدیگر متصل می شوند تشکیل یک شبکه از شبکه ها یا شبکه متصل را می دهند. همچنین می توان شبکه ای که از اتصال داخلی میان شبکه های عمومی، خصوصی، تجاری، صنعتی یا دولتی به وجود می آید را شبکه متصل نامید.

در کاربردهای جدید، شبکه های به هم متصل شده از قرارداد IP استفاده می کنند. بسته به اینکه چه کسانی یک شبکه را مدیریت می کنند و اینکه چه کسانی در این شبکه عضو هستند، می توان سه نوع شبکه متصل دسته بندی نمود:

- **شبکه داخلی یا اینترانت (Intranet)**

- **شبکه خارجی یا اکسترانت (Extranet)**
- **شبکه اینترنت (Internet)**

شبکه های داخلی یا خارجی ممکن است که اتصالاتی به شبکه اینترنت داشته و یا نداشته باشند. در صورتی که این شبکه ها به اینترنت متصل باشند در مقابل دسترسی های غیرمجاز از سوی اینترنت محافظت می شوند. خود شبکه اینترنت به عنوان بخشی از شبکه داخلی یا شبکه خارجی به حساب نمی آید، اگرچه که ممکن است شبکه اینترنت به عنوان بستری برای برقراری دسترسی بین قسمت هایی از یک شبکه خارجی خدماتی را ارائه دهد.

۱- شبکه داخلی (Intranet)

یک شبکه داخلی مجموعه ای از شبکه های متصل به هم می باشد که از قرارداد IP و ابزارهای مبتنی بر IP مانند مرورگر های وب استفاده می کند و معمولاً زیر نظر یک نهاد مدیریتی کنترل می شود. این نهاد مدیریتی شبکه داخلی را نسبت به باقی قسمت های دنیا محصور می کند و به کاربران خاصی اجازه ورود به این شبکه را می دهد. به طور معمول تر شبکه درونی یک شرکت یا دیگر شرکت ها شبکه داخلی می باشد.

۲- شبکه خارجی (Extranet)

یک شبکه خارجی یک شبکه یا یک شبکه متصل است که به لحاظ قلمرو محدود به یک سازمان یا نهاد است ولی همچنین شامل اتصالات محدود به شبکه های متعلق به یک یا چند سازمان یا نهاد دیگر است که معمولاً، ولی نه همیشه، قابل اعتماد هستند. برای نمونه مشتریان یک شرکت ممکن است که دسترسی به بخش هایی از شبکه داخلی آن شرکت داشته باشند که بدین ترتیب یک شبکه خارجی درست می شود، چراکه از نقطه نظر امنیتی این مشتریان برای شبکه قابل اعتماد به نظر نمی رسند. همچنین از نظر فنی می توان یک شبکه خارجی را در گروه شبکه های دانشگاهی، کلان شهری، گسترده یا دیگر انواع شبکه (هر چیزی غیر از شبکه محلی) به حساب آورد، چراکه از نظر تعریف یک شبکه خارجی نمی تواند فقط از یک شبکه محلی تشکیل شده باشد، چون بایستی دست کم یک اتصال به خارج از شبکه داشته باشد.

۳- شبکه اینترنت (Internet)

شبکه ویژه ای از شبکه ها که حاصل اتصالات داخلی شبکه های دولتی، دانشگاهی، عمومی و خصوصی در سرتاسر دنیا است. این شبکه بر اساس شبکه اولیه ای کار می کند که آرپانت (ARPANET) نام داشت و به وسیله موسسه آرپا (ARPA) که وابسته به وزارت دفاع ایالات متحده آمریکا است ایجاد شد. همچنین منزلگاهی برای وب جهان گستر (WWW) است. در لاتین واژه Internet برای نامیدن آن بکار می رود که برای اشتباه نشدن با معنی عام واژه شبکه متصل حرف اول را بزرگ می نویسند.

۱-۶-۵- بر اساس لایه شبکه

ممکن است شبکه های رایانه ای مطابق مدلهای مرجع پایه ای که در صنعت به عنوان استاندارد شناخته می شوند مانند مدل مرجع ۷ لایه OSI و مدل ۴ لایه TCP/IP، بر اساس نوع لایه شبکه ای که در آن عمل می کنند طبقه بندی شوند. این دو مورد در فصلی جداگانه بررسی می شوند.

۱-۶-۶- بر اساس معماری کاربری

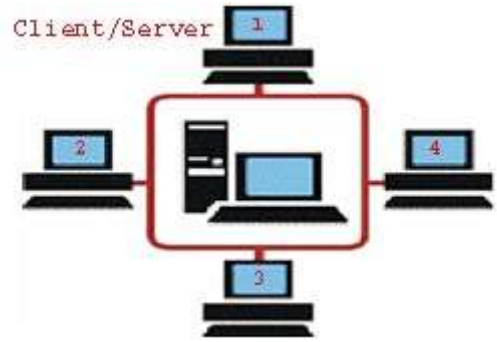
ممکن است شبکه های رایانه ای بر اساس معماری کاربری که بین اعضای شبکه وجود دارد طبقه بندی شود، برای نمونه معماری های Active Networking، مشتری-خدمت گذار (Client-Server) و همتا به همتا Peer-to-Peer (گروه کاری).

۱. **شبکه های نقطه به نقطه (Peer to Peer)** که نام دیگر آنها WORK GROUP می باشد.

در مدل Peer-to-Peer هر کاربری میتواند فایلها را با دیگر کاربران بدون نیاز به یک سرور مرکزی و خاص، به اشتراک بگذارد.

۲. **شبکه های مبتنی بر سرور (Server Based)** که به آنها Client / Server نیز می گویند.

در شبکه Client/Server یک یا چند کامپیوتر به عنوان سرویس دهنده (سرور) برای اشتراک فایلها، منابع و برنامه ها وجود دارد.



۱-۶-۷- بر اساس همبندی (توپولوژی)

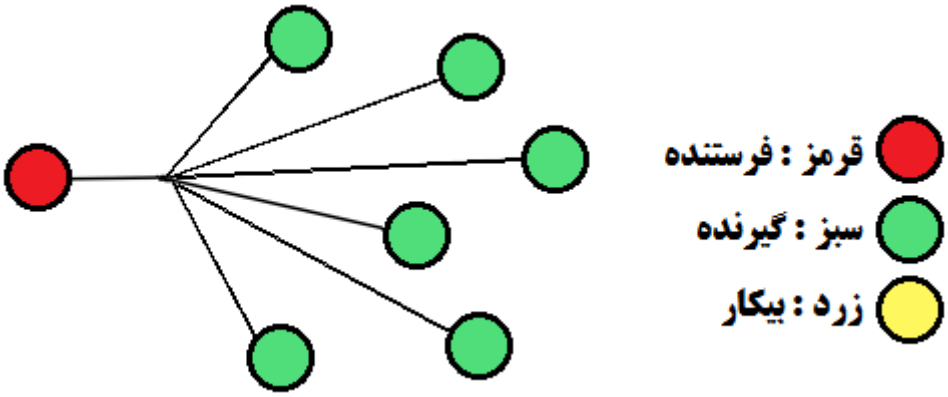
ممکن است شبکه های رایانه ای بر اساس نوع همبندی شبکه طبقه بندی شوند مانند: شبکه خطی (Bus)، شبکه ستاره (Star)، شبکه حلقه ای (Ring)، شبکه توری (Mesh)، شبکه ستاره-باس (Star-Bus)، شبکه درختی (Tree) یا شبکه سلسله مراتبی (Hierarchical) و غیره.

همبندی شبکه را می توان بر اساس نظم هندسی ترتیب داد. همبندی های شبکه طرح های منطقی شبکه هستند. واژه منطقی در اینجا بسیار پرمعنی است. این واژه به این معنی است که همبندی شبکه به طرح فیزیکی شبکه بستگی ندارد. مهم نیست که رایانه ها در یک شبکه به صورت خطی پشت سر هم قرار گرفته باشند، ولی زمانیکه از طریق یک هاب به یکدیگر متصل شده باشند تشکیل همبندی ستاره می کنند نه باس. و این عامل مهمی است که شبکه ها در آن فرق می کنند، جنبه ظاهری و جنبه عملکردی. توپولوژی ها در فصلی جداگانه بررسی می شوند.

۱-۶-۸- بر اساس مسیر دهی بسته ها

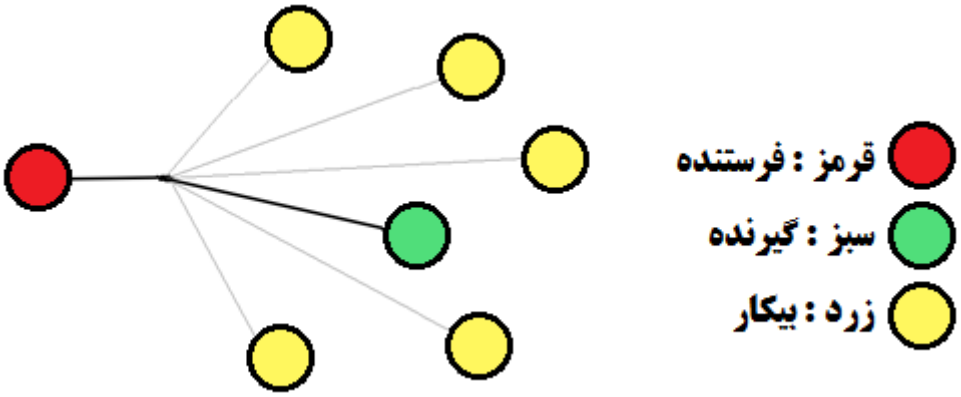
۱. Broadcast Network

در اتصال Broadcast Network هر کامپیوتر توسط Node کابل شبکه خود همواره باید یا بطور مستقیم به کامپیوتر دیگر متصل بوده و یا توسط یک رسانه Media همانندHub به کامپیوتر دیگر متصل شود. در این روش کامپیوتر پیغام دهنده Packet اطلاعات خود را در کل رسانه رها می نماید با این توضیح که نام و آدرس کامپیوتر پیغام گیرنده را هم به همراه آن ارسال می کند. این Packet به همه کامپیوتر ها رسیده و تنها توسط کامپیوتری دریافت و خوانده می شود که آدرس و نام کامپیوتری که همراه با Packet ارسال شده است - با آن همخوانی داشته باشد. در این ساختار علاوه بر اینکه ترافیک شبکه زیاد بوده و باعث کم شدن سرعت کارکرد شبکه می شود امنیت آن نیز از سطح مطلوبی برخوردار نیست. زیرا Packet اطلاعات که ممکن است محرمانه هم باشد در سطح شبکه پخش شده و به همه کامپیوتر ها می رسد. این ساختار از پیچیدگی کمتری برخوردار بوده و هزینه تهیه سخت افزارهای لازم برای راه اندازی آن کم است.



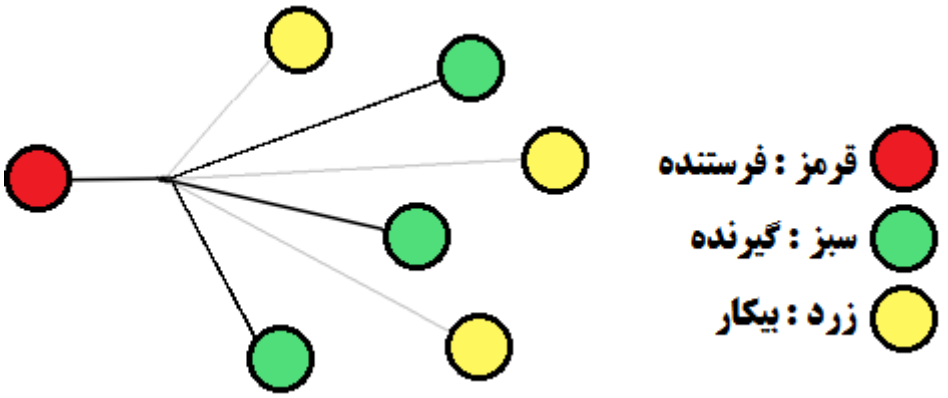
۲. (Unicast) Point to Point Network

در اتصال Point to Point Network دریافت و ارسال Packet ها در شبکه توسط ابزاری هوشمند کنترل می شود بگونه ای که Packet اطلاعاتی که برای یک کامپیوتر مشخص ارسال می گردد تنها به سمت همان کامپیوتر ارسال شده و دیگر کامپیوتر ها امکان دسترسی به آن را ندارند از طرف دیگر به دلیل اینکه این بسته اطلاعاتی در کل شبکه منتشر نمی شود. ترافیک شبکه بطور قابل ملاحظه ای پایین آمده و امنیت درسطح شبکه بالا می رود. اینگونه شبکه ها به دلیل داشتن ابزاری چون سوئیچ های هوشمند گران تر از نوع قبل می باشد.



۳. Multicast Network

در این روش، کامپیوتر ارسال کننده، بسته ها را نه به تمامی کامپیوتر های موجود ارسال می کند و نه به یک تک کامپیوتر خاص؛ بلکه در این روش، کامپیوتر ارسال کننده، از بین کامپیوتر های موجود، تعدادی را انتخاب کرده و بسته ها را به سمت آن ها ارسال می کند. مثلاً بسته ها را به سمت کامپیوتر های با شماره زوج یا کامپیوتر های با حافظه RAM بیشتر از 2 GB می فرستد. در این روش، فرآیند ارسال به کمک الگویی خاص (Pattern) انجام می گیرد.

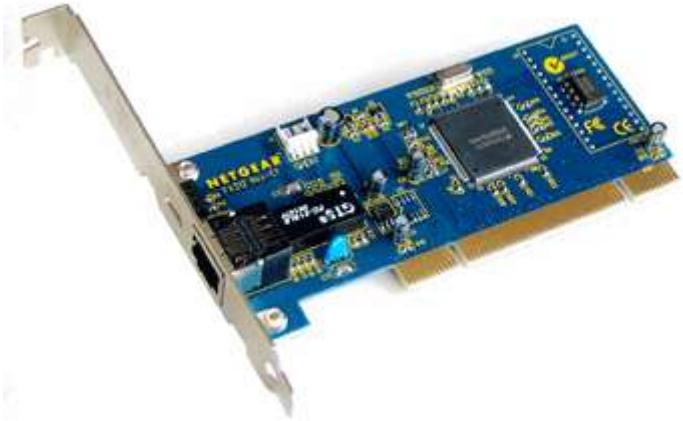


۱-۷- اجزای اصلی سخت افزاری

همه شبکه ها از اجزای سخت افزاری پایه ای تشکیل شده اند تا گره های شبکه را به یکدیگر متصل کنند، مانند کارت های شبکه، تکرارگر ها، هاب ها، پلها، راهگزین ها (Switch) و مسیریاب ها. علاوه بر این، روشهایی برای اتصال این اجزای سخت افزاری لازم است که معمولاً از کابل های الکتریکی استفاده می شود. (از همه رایجتر کابل رده ۵ (کابل Cat5) است)، و کمتر از آنها، ارتباطات مایکروویو (مانند IEEE 802.11) و (کابل فیبر نوری Optical Fiber Cable) بکار می روند.

۱-۷-۱- کارت شبکه (NIC)

کارت شبکه، آداپتور شبکه یا کارت واسط شبکه (Network Interface Card) قطعه ای از سخت افزار رایانه است و طراحی شده تا این امکان را به رایانه ها بدهد که بتوانند بر روی یک شبکه رایانه ای با یکدیگر ارتباط برقرار کنند. این قطعه دسترسی فیزیکی به یک رسانه شبکه را تامین می کند و با استفاده از آدرس های MAC، سیستمی سطح پایین جهت آدرس دهی فراهم می کند. این شرایط به کاربران اجازه می دهد تا به وسیله کابل یا به صورت بی سیم به یکدیگر متصل شوند.



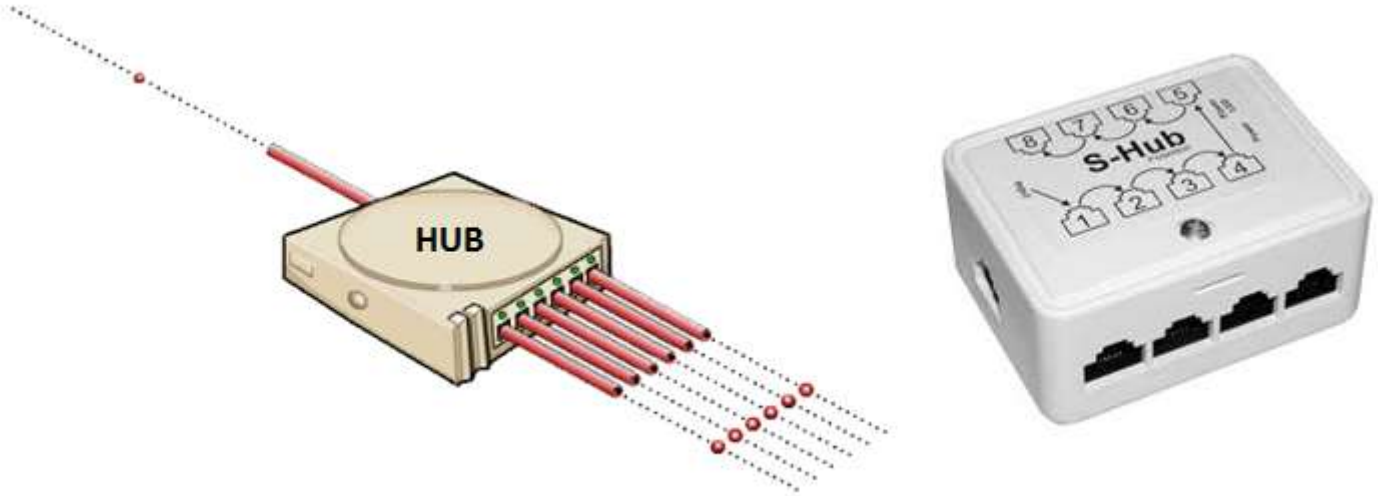
۱-۷-۲- تکرارگر (Repeater)

تکرارگر تجهیزی الکترونیکی است که سیگنالی را دریافت کرده و آن را با سطح دامنه بالاتر، انرژی بیشتر و یا به سمت دیگر یک مانع ارسال می کند. بدین ترتیب می توان سیگنال را بدون کاستی به فواصل دورتری فرستاد. از آنجا که تکرارگر ها با سیگنال های فیزیکی واقعی سروکار دارند و در جهت تفسیر داده ای که انتقال می دهند تلاشی نمی کنند، این تجهیزات در **لایه فیزیکی** یعنی اولین لایه از مدل مرجع OSI عمل می کنند.

۱-۷-۳- هاب (جعبه تقسیم)

هاب قطعه ای سخت افزاری است که امکان اتصال قسمت های یک شبکه را با هدایت ترافیک در سراسر شبکه فراهم می کند. هاب ها در **لایه فیزیکی** از مدل مرجع OSI عمل می کنند. عملکرد هاب بسیار ابتدایی است، به این ترتیب که داده رسیده از

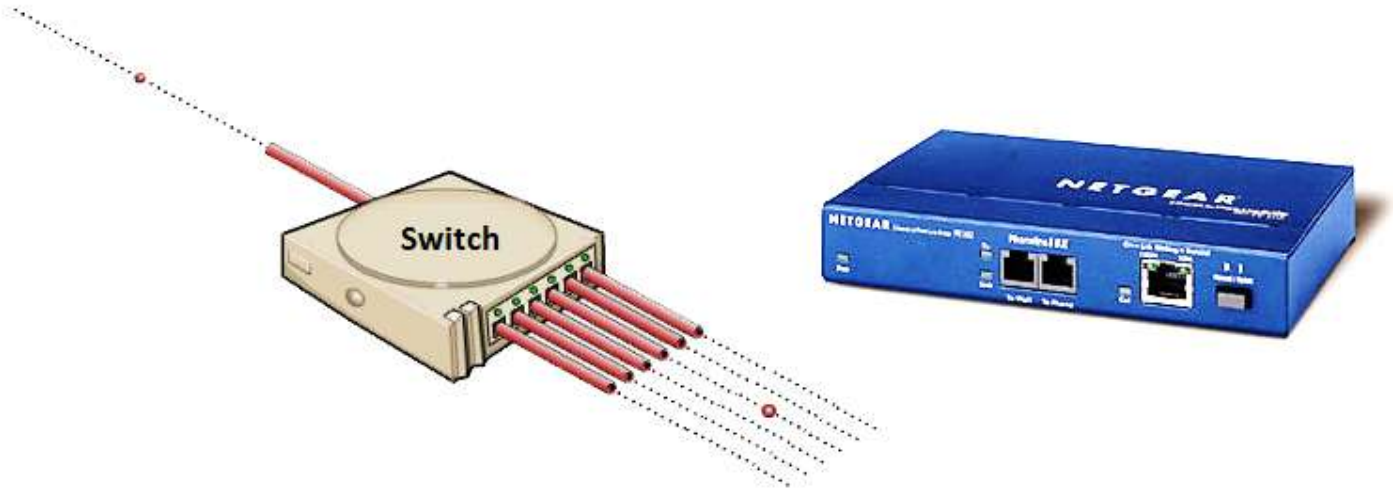
یک گره را برای تمامی گره های شبکه کپی می کند. هاب ها مانند تکرارگر ها، عملیات تقویت سیگنال را نیز انجام می دهند. هاب ها عموماً برای متصل کردن بخش های یک شبکه محلی بکار می روند. هر هاب چندین درگاه (پورت) دارد. زمانی که بسته ای از یک درگاه می رسد، به دیگر درگاه ها کپی می شود، بنابراین همه قسمت های شبکه محلی می توانند بسته ها را ببینند.



۱-۷-۴- راهگزین (Switch)

راهگزین که در پارسی بیشتر واژه سوئیچ برای آن بکار برده می شود، وسیله ای است که قسمت های شبکه را به یکدیگر متصل می کند. راهگزین های معمولی شبکه تقریباً ظاهری شبیه به هاب دارند، ولی یک راهگزین در مقایسه با هاب از هوشمندی بیشتری (و همچنین قیمت بیشتری) برخوردار است. راهگزین های شبکه این توانمندی را دارند که محتویات بسته های داده ای که دریافت می کنند را بررسی کرده، دستگاه فرستنده و گیرنده بسته را شناسایی کنند، و سپس آن بسته را به شکلی مناسب ارسال نمایند. با ارسال هر پیام فقط به دستگاه متصلی که پیام به هدف آن ارسال شده، راهگزین پهنای باند شبکه را به شکل بهینه تری استفاده می کند و عموماً عملکرد بهتری نسبت به یک هاب دارد.

از نظر فنی می توان گفت که راهگزین در لایه پیوند داده از مدل مرجع OSI عمل کنند. ولی بعضی انواع راهگزین قادرند تا در لایه های بالاتر نیز به بررسی محتویات بسته بپردازند و از اطلاعات بدست آمده برای تعیین مسیر مناسب ارسال بسته استفاده کنند. به این راه گزین ها به اصطلاح راهگزین های چندلایه (Multilayer Switch) می گویند.



۱-۷-۵- پل (Bridge)

یک پل دو زیر شبکه (سگمنت) را در لایه پیوند داده از مدل مرجع OSI به هم متصل می کند. پل ها شبیه به تکرارگر ها و هاب های شبکه اند که برای اتصال قسمت های شبکه در لایه فیزیکی عمل می کنند، با این حال پل با استفاده از مفهوم پل

زدن کار می کند، یعنی به جای آنکه ترافیک هر شبکه بدون نظارت به دیگر درگاه ها کپی شود، آنرا مدیریت می کند. بسته هایی که از یک طرف پل وارد می شوند تنها در صورتی به طرف دیگر انتشار می یابند که آدرس مقصد آن ها مربوط به سیستم هایی باشد که در طرف دیگر پل قرار دارند. پل مانع انتشار پیغام های همگانی در قطعه های کابل وصل شده به آن نمی شود. **در اصل می توان گفت که وظیفه پل، اتصال سگمنت های مختلف شبکه می باشد. منظور از سگمنت می تواند شبکه های با معماری مختلف یا شبکه های با آدرس مختلف باشد.**

البته گاهی از پل به عنوان دروازه (Gateway) یاد می کنند.Gateway، کامپیوتری است که بسته های خارج شده از هر کامپیوتر ابتدا به سمت آن می رود. البته پل برای اتصال شبکه های نا همگون نیز به کار می رود.

پل ها به سه دسته تقسیم می شوند:

پل های محلی: مستقیماً به شبکه های محلی متصل می شود.

پل های دوردست: از آن می توان برای ساختن شبکه های گسترده جهت ایجاد ارتباط بین شبکه های محلی استفاده کرد. پل های دور دست در شرایطی که سرعت اتصال از شبکه های انتهایی کمتر است با مسیریابها جایگزین می شوند.

پل های بی سیم: برای اتصال شبکه های محلی به شبکه های محلی بی سیم یا شبکه های محلی بی سیم به هم یا ایستگاه های دوردست به شبکه های محلی استفاده می شوند.

۱-۷-۶- مسیریاب (Router)

مسیریاب ها تجهیزات شبکه ای هستند که بسته های داده را با استفاده از سرآیند ها (Header) و جدول ارسال تعیین مسیر کرده، و ارسال می کنند. مسیریاب ها در لایه شبکه از مدل مرجع OSI عمل می کنند. همچنین مسیریاب ها اتصال بین بستر های فیزیکی متفاوت را امکان پذیر می کنند. این کار با چک کردن سرآیند یک بسته داده انجام می شود. مسیر یاب ها قادر به انتقال داده ها به صورت Broadcast نیستند.

مسیریاب ها از قراردادهای مسیر یابی مانند OSPF استفاده می کنند تا با یکدیگر گفتگو کرده و بهترین مسیر بین هر دو ایستگاه را پیکربندی کنند. هر مسیریاب دسته کم به دو شبکه، معمولاً شبکه های محلی، شبکه های گسترده و یا یک شبکه محلی و یک سرویس دهنده اینترنت متصل است. بعضی انواع مودم های DSL و کابلی جهت مصارف خانگی درون خود از وجود یک مسیریاب نیز بهره می برند.

۱-۸- سیستم های شبیه به شبکه

گاهی اوقات می توان کامپیوتر ها را به شکلی بکار برد که دقیقا با یک شبکه سر و کار نداریم اما می توان آنها را شبکه نیز به حساب آورد. به همین دلیل نام آنها را سیستم های شبیه شبکه می نامیم و در زیر آنها را توضیح می دهیم. اما قبل از آن باید با مفهوم کامپیوتر Standalone آشنا شوید. به طور کلی به کامپیوتر های که قادر باشیم پشت آنها قرار گیریم و با آنها کار انجام دهیم خواه به شبکه متصل نباشد یا امکان آن را نداشته باشد یک کامپیوتر Standalone گوییم.

سیستم های شبیه شبکه، بطور کلی سه مورد می باشند:

۱-۸-۱- کامپیوتر های Mainframe

این کامپیوتر ها دارای چندین پردازنده و حافظه های بزرگ می باشند و ترمینال ها که فقط دارای مانیتور و صفحه کلید می باشند به آن متصل می شوند و از آن استفاده می کنند. پس به نوعی می توان آنها را نوعی شبکه نامید اما نه بطور کامل.

۱-۸-۲- Distributed System (سیستم های توزیع شده)

این سیستم های شامل چندین کامپیوتر جداگانه می باشند که بر روی همه آنها یک سیستم عامل مخصوص مانند ماخ (Mach) نصب می شود و این سیستم عامل است که کلیه پردازش ها را مدیریت می کنند و تصمیم می گیرد که مثلاً این برنامه روی کدام سیستم ها انجام شود و یا مثلاً این داده روی کدام سیستم ها ذخیره شود و در این موارد کاربر نمی تواند هیچ کاری انجام دهد. این کامپیوتر ها بیشتر برای انجام پردازش های بسیار سنگین و به صورت موازی بکار می روند.

۱-۸-۳- کامپیوتر هایی که به یکدیگر link می شوند

یکی از راههایی که می توان کامپیوتر ها را به یکدیگر متصل کرد از طریق پورت های پشت آنها می باشد. اگر دو کامپیوتر را بتوان از طریق پورت های پشت آنها به یکدیگر متصل کرد در اصطلاح آنها را لینک کرده ایم. در سیستم عامل ویندوز نیز می توانید دو کامپیوتر را بدین روش به یکدیگر متصل کنید. برای اینکار در موقع نصب ویندوز باید نرم افزار آن را نصب کنید تا بتوانید دو کامپیوتر را در قالب Host و Guest استفاده نمایید

۱-۹- مراحل راه اندازی یک شبکه

برای راه اندازی هر نوع شبکه ای مراحل زیر را باید طی کرد.

۱. طراحی (Design)
۲. تنظیمات (Roll Out)
۳. پیکربندی (Configuration)
۴. مدیریت (Management)

۱-۹-۱- طراحی شبکه (Design)

فاز طراحی معمولاً یک الی سه روز طول میکشد که بستگی به بزرگی شبکه و کار آن دارد.

نکاتی که در فاز طراحی باید به آنها توجه کرد:

۱. شبکه Peer-to-Peer است یا Client/Server

۲. انتخاب نرم افزار شبکه
۳. انتخاب زبان شبکه
۴. تهیه لیست سخت افزارهای موردنیاز
۵. تعیین میزان سطح امنیت اطلاعات
۶. یادگیری راه حل های نرم افزاری و سخت افزاری برای رفع مشکلات مدیریتی روزمره

۱-۹-۲- تنظیمات شبکه (Roll Out)

برای تنظیم کردن شبکه مراحل زیر را باید انجام داد:

۱. آزمایش کابل ها
۲. نصب یک یا چند سِرور، اگر شبکه از نوع مدل Client/Server باشد.
۳. نصب سخت افزار کامپیوتر های دیگر (گروه کاری)
۴. اتصال کارت های شبکه به کابل ها (NIC-کارت شبکه باعث اتصال کامپیوتر ها به شبکه می شود.)
۵. نصب یک یا چند Hub (اگر از کابل Twisted Pair استفاده می شود. در این نوع شبکه ها از توپولوژی Star استفاده می شود.)
۶. نصب چاپگر ها
۷. نصب برنامه سرویس دهنده (سیستم عامل شبکه یا NOS) اگر مدل شبکه Client/Server است
۸. نصب برنامه روی کامپیوتر های دیگر
۹. نصب برنامه های کاربردی

۱-۹-۳- پیکربندی شبکه (Configuration)

پیکربندی شبکه به معنای سفارشی کردن آن برای کاربر است.

۱. ایجاد حساب های دسترسی به شبکه برای کاربران (نام کاربری- کلمه عبور- گروه کاری)
۲. تخصیص فضایی از هارد دیسک برای به اشتراک گذاشتن فایلها و داده های کاربران
۳. تخصیص فضایی از هارد دیسک برای به اشتراک گذاشتن برنامه ها توسط کاربران
۴. تنظیم نوبت چاپ (نرم افزاری که اجازه میدهد کاربران از چاپگر های شبکه استفاده کنند)
۵. نصب سیستم پشتیبانی شبکه برروی ایستگاه های کاری کاربران

۱-۹-۴- مدیریت و اداره شبکه (Management)

۱. نقشه برداری از شبکه به منظور مدیریت و اشکال زدایی آسانتر
۲. نصب سطوح امنیتی مناسب به منظور جلوگیری از خسارات عمدی و سهوی
۳. بالا بردن سرعت شبکه از طریق تنظیم LAN
۴. ایجاد استانداردهای شرکت برای اضافه کردن سخت افزار و نرم افزار. با این کار میتوان از بروز مشکلات در آینده جلوگیری کرد.

فصل ۲

آدرس IP

۲-۱- آدرس IP چیست؟

یکی از سوالاتی که معمولاً پیش می آید این است که "آدرس IP چیست؟" آدرس IP، شماره شناسایی هر کامپیوتر متصل به شبکه است. بنابر این می توان گفت که IP، شماره شناسایی هر کاربر شبکه است.

نشانی پروتکل اینترنت (Internet Protocol Address) یا به اختصار آدرس IP (IP Address) نشانی عددی است که به هریک از دستگاه ها و رایانه های متصل به شبکه ی رایانه ای که بر مبنای مدل مرجع TCP/IP (از جمله اینترنت) کار می کند، اختصاص داده می شوند. پیام هایی که دیگر رایانه ها برای این رایانه می فرستند با این نشانه ی عددی همراه است و مسیر یاب های شبکه آن را مانند نشانی گیرنده در نامه های پستی تعبیر می کنند، تا بالاخره پیام به شبکه رایانه مورد نظر برسد.

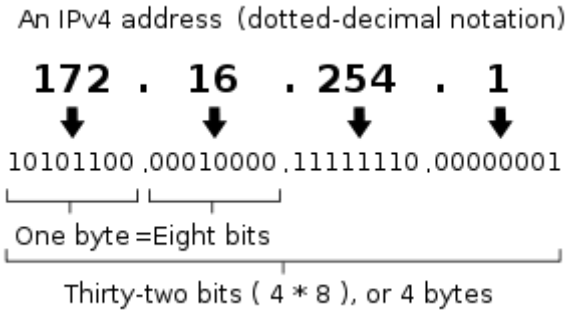
آدرس IP را می توان با شماره تلفن های افراد در شبکه تلفن مقایسه کرد. البته تفاوت های زیادی بین آدرس IP و شماره تلفن ها وجود دارد. ولی همانند آن، پیش شماره دارد و وقتی کامپیوتری متصل به شبکه اینترنت است، این آدرس انحصاری بوده و فقط در اختیار آن کامپیوتر قرار دارد. تفاوت مهم آن با شماره تلفن ها در این است که چنانکه به هر دلیلی (ارادی و یا غیر ارادی) کامپیوتری که این شماره (IP) به آن تخصیص داده شده، از شبکه اینترنت جدا شود (ارتباطش قطع گردد) این IP آزاد شده و ممکن است به کامپیوتر دیگری تخصیص داده شود.

البته در اینجا باز نکته مهمی وجود دارد: شماره IP برای کامپیوتر های سرور شبکه (کامپیوتر هایی که به شبکه سرویس می دهند و شبکه را تحت نظارت مستمر خود دارند) و نیز کامپیوتر هایی که به روشی غیر از روش شماره گیری تلفنی (Dial Up) به اینترنت وصل هستند (کامپیوتر های کلاینت) معمولاً عددی ثابت بوده و تغییر نمی کند. ولی همانطوری که اشاره شد برای دیگر کامپیوتر ها، عددی متغیر است و در هر بار اتصال به اینترنت ممکن است این شماره عوض شود. یعنی هر بار که شما با شرکت ISP خود تماس می گیرید و از طریق آن به شبکه اینترنت وصل می شوید، عددی جدید (از مجموعه شماره های IP آزاد در آن موقع) به کامپیوتر شما تخصیص داده می شود.

۲-۲- انواع IP

در حال حاضر، دو نسخه IP درحال استفاده می باشد: IP نسخه ۴ و IP نسخه ۶ که هر یک نشانی IP را به روش متفاوتی ارائه می نمایند.

۲-۳- آدرس IP نسخه ۴



آدرس IP نسخه ۴، یک عدد ۳۲ بیتی است که برای سادگی آن را به شکل چهار بخش عددی در مبنای ده می نویسند که با نقطه از هم جدا می شوند (مانند ۱۹۹.۲۱۱.۴۵.۵). این روش نشانی دهی را ده دهی نقطه دار می نامند. هر یک از چهار بخش را یک هشتایی (Octet) می گویند، زیرا طول آن ۸ بیت (یا ۱ بایت) است و می تواند عددی از ۰ تا ۲۵۵ باشد. پس ۲ به توان ۳۲ آدرس مختلف یا به عبارتی ۴.۲۹۴.۹۶۷.۲۹۶ آدرس متمایز داریم.

اصولاً هر نشانی IP که ۳۲ بیتی است، به دو بخش تقسیم می شود: **یک پیشوند** و **یک پسوند**. این دو سطح به منظور ایجاد یک روش مسیر یابی کارآمد طراحی شده است. پیشوند، آدرس شبکه ای که رایانه به آن متصل است را مشخص می کند (Network). در حالیکه پسوند، یک رایانه یکتا را روی شبکه مشخص می کند (Host)؛ یعنی به هر شبکه در اینترنت، یک مقدار یگانه که تحت عنوان شماره شبکه شناخته شده است، اختصاص دارد. شماره شبکه به عنوان یک پیشوند در نشانی هر رایانه ای که به شبکه وصل است ظاهر می شود. بعلاوه به هر رایانه روی یک شبکه، یک پسوند نشانی یکتا تخصیص یافته است.

هر نشانی کامل، شامل یک پیشوند و یک پسوند است و طوری تخصیص داده می شوند که یکتا باشند، بنابراین ویژگی اول تضمین می گردد. اگر دو رایانه به دو شبکه مختلف وصل شده باشند، نشانی هایشان پیشوند های متفاوت خواهند داشت. اما اگر دو رایانه به یک شبکه وصل باشند، نشانی هایشان دارای پسوندهای متفاوت خواهد بود.

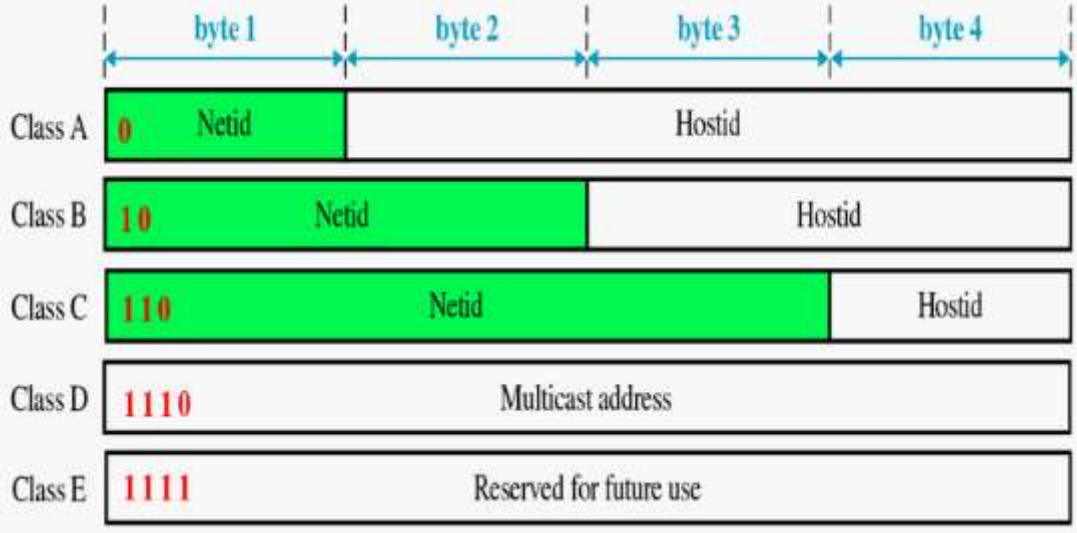
۲-۳-۱- کلاس های مختلف IP نسخه ۴

سه کلاسِ پایه ای مختلفِ نشانی دهی IP، برای شبکه های بزرگ، متوسط و کوچک (از نظر تعداد کامپیوتر در یک شبکه)، وجود دارد. کلاس A برای شبکه های بزرگ، کلاس B برای شبکه های متوسط و کلاس C برای شبکه های کوچک است. علاوه بر این سه کلاس، کلاس D برای پخش چندگانه ارسال اطلاعات به گروهی از رایانه ها، و کلاس E برای کارهای جستجو و تحقیقاتی وجود دارد. برای شرکت در پخش چندگانه IP، مجموعه ای از رایانه های میزبان باید بر سر استفاده از آدرس پخش چندگانه، به طور مشترک توافق داشته باشند. پس از تشکیل گروه پخش چندگانه یک کپی از هر بسته اطلاعاتی فرستاده شده به نشانی پخش چندگانه به هر رایانه میزبان در مجموعه تحویل می گیرد. نخستین ۴ بیت (از سمت چپ) آدرس IP کلاس آن را مشخص می کند. همچنین اگر نمایش نقطه دار را در نظر بگیریم از روی مقدار ده دهی بایت اول کلاس آن تشخیص داده می شود:

کلاس	بیت آغازین	شروع	پایان	CIDR	Subnet Mask
Class A	۰	۰.۰.۰.۰	۱۲۷.۲۵۵.۲۵۵.۲۵۵	۸/	۲۵۵.۰.۰.۰
Class B	۱۰	۱۲۸.۰.۰.۰	۱۹۱.۲۵۵.۲۵۵.۲۵۵	۱۶/	۲۵۵.۲۵۵.۰.۰
Class C	۱۱۰	۱۹۲.۰.۰.۰	۲۲۳.۲۵۵.۲۵۵.۲۵۵	۲۴/	۲۵۵.۲۵۵.۲۵۵.۰

Not Defined	۴/	۲۳۹.۲۵۵.۲۵۵.۲۵۵	۲۲۴.۰.۰.۰	۱۱۱۰	**Class D** [multicast]
Not Defined	۴/	۲۵۵.۲۵۵.۲۵۵.۲۵۵	۲۴۰.۰.۰.۰	۱۱۱۱	**Class E** [reserved]

شکل زیر تصویر بهتری از کلاس های آدرس IP به شما می دهد:



تصویر زیر نیز محدوده هر کلاس IP را نشان می دهد:

اصولا در سامانه IP دهی به مشترکان، IP ها به صورت تعدادی که توانی از عدد ۲ باشد (۲، ۴، ۸، ۱۶، ۳۲، ۶۴ و ۱۲۸) دسته بندی می شوند. لازم به ذکر است که در هر دسته IP اختصاص داده شده به مشترک، IP های اول و آخر بر اساس استاندارد معمولاً غیر قابل استفاده است و از باقیمانده IP ها می توان در شبکه محصور شده استفاده کرد. به عنوان مثال در یک کلاس هشت تایی، حداکثر شش نشانی IP قابل استفاده است. این بدین دلیل است که آدرس کامپیوتر در شبکه (پسوند) نمی تواند تماما ۱ یا تماما ۰ باشد. بنابراین تعداد ۲ تا از IP های قابل تخصیص در هر شبکه کم می شود.

۲-۳-۲- IP خصوصی

برای جلوگیری از هدر دهی IP در هر کلاس، یک محدوده IP برای شبکه های خصوصی (مانند شبکه داخلی ادارات و شرکت ها) در نظر گرفته شده است. این آدرس ها قابل استفاده در شبکه اینترنت نمی باشد و معمولاً در شبکه های خصوصی و محلی استفاده می شود. این آدرس ها عبارتند از:

کلاس	تعداد آدرس ها	محدوده IP
Class A	۱۶,۷۷۷,۲۱۶	۱۰.۰.۰.۰ تا ۱۰.۲۵۵.۲۵۵.۲۵۵
Class B	۱,۰۴۸,۵۷۶	۱۷۲.۱۶.۰.۰ تا ۱۷۲.۳۱.۲۵۵.۲۵۵

۱۹۲.۱۶۸.۰.۰ تا ۱۹۲.۱۶۸.۲۵۵.۲۵۵	۶۵,۵۳۶	Class C

برای اتصال یک شبکه خصوصی به اینترنت از پروتکل NAT (Network Address Translation) استفاده می شود به این ترتیب که **نشانی خصوصی** به یک یا چند نشانی **منحصر به فرد عمومی** ترجمه می شود.

نام دیگر IP خصوصی، IP Invalid است. یعنی نمی توان در شبکه اینترنت از آن ها برای آدرس Serverها استفاده کرد. نقطه مقابل IP خصوصی، IP عمومی (Public) یا Valid IP قرار دارد که برای آدرس دهی Host های اینترنت از آن ها استفاده می شود.

۲-۳-۳- NAT چیست؟ (Network Address Translation)

می دانیم که هر کامپیوتری که قصد استفاده از اینترنت را دارد، بایستی یک آدرس Valid داشته باشد تا بتواند از خدمات اینترنت استفاده کند. بدین معنا که مثلاً اگر کامپیوتری درخواست مشاهده سایت http://www.google.com را نمود، صفحه باز شده (نتیجه کار نه درخواست انجام کار)، بایستی به کدام یک از کامپیوترهای متصل به اینترنت ارسال شود؟ یعنی کامپیوتر شما چگونه بایستی شناسایی شود؟ بنابراین بایستی کامپیوتر شما به صورت یکتا در اینترنت شناخته گردد. اما متاسفانه به تعداد کافی آدرس IP برای تخصیص به تمامی کامپیوتر ها و تجهیزات متصل به اینترنت و یکتا نمودن آن ها در اینترنت وجود ندارد. راه حل چیست؟

راه حل این است که دستگاهی خاص یا کامپیوتری خاص که یک آدرس IP به صورت Valid دارد و در سطح دنیا نیز شناخته می شود، نقش NAT Server را بازی نموده و کار ترجمه آدرس را انجام دهد. روال کار بدین صورت خواهد بود که به جای اینکه شما، آدرس IP به صورت Valid داشته باشید و به صورت مستقیم به اینترنت وصل شوید، شما به NAT Server متصل می شوید و درخواست های اینترنت خود را به آن می دهید. این سرور که یک آدرس Valid دارد نیز درخواست های شما را به سمت اینترنت می دهد و پاسخ دریافت شده را به شما باز می گرداند. بدین ترتیب شما نیازی به داشتن آدرس Valid نخواهید داشت. در واقع با این کار، NAT Server، یک آدرس Valid را با چند کامپیوتر متصل به آن، به اشتراک می گذارد.

مثلاً زمانی که به صورت Dial-UP به اینترنت متصل می شوید، درخواست های اینترنت خود را به کامپیوتری در ISP ارائه دهنده خدمات اینترنت خود می دهید. این کامپیوتر نیز درخواست های شما را به سمت اینترنت فرستاده و پاسخ دریافت شده را به سمت شما باز می گرداند.

NAT Server هم به صورت سخت افزاری (تجهیزی جداگانه) و هم به صورت نرم افزاری (ویندوز سرور) قابل پیاده سازی است که نوع نرم افزاری آن را در فصول انتهایی همین جزوه و در قسمت VPN Server آموزش خواهیم داد.

۲-۳-۴- IP ایستا و پویا

IP پویا با هر بار وصل شدن به شبکه داخلی و یا اینترنت تغییر می کند. اما IP ایستا (Static) اینطور نیست. IP پویا (Dynamic) در هر شبکه توسط سرور پروتکل پیکربندی پویای میزبان (DHCP Server) به رایانه ها در شبکه اختصاص داده می شود. یعنی وقتی شما به اینترنت و یا شبکه داخلی وصل می شوید، سرور پروتکل پیکربندی پویای میزبان به شما یک نشانی IP اختصاص می دهد.

DHCP Server می تواند یک سرویس در سیستم عامل های سرور باشد یا یک قطعه سخت افزاری مانند مسیریاب (Router) و یا نقطه دسترسی (Access Point) در شبکه باشد.

برای دیدن نشانی IP رایانه خود می توان از برنامه winipcfg.exe (در ویندوز ۹۵ و ۹۸ و ME) یا ipconfig.exe (در ویندوز ۲۰۰۰ و XP و Vista و ۷) استفاده کرد (با تایپ دستور در Command Prompt). در لینوکس یا یونیکس (یا سیستم های مبتنی بر آن ها) نیز می توان از دستور ifconfig استفاده کرد.

۲-۴- آدرس IP نسخه ۶

گسترش روز افزون اینترنت و نیاز به آدرس های بسیار بیشتر تیم Internet Engineering Task Force را برآن داشت تا به فکر تکنولوژی های جدیدی باشند تا امکان تعریف آدرس های IP بیشتری فراهم گردد. بهترین راه ساخت مجدد نشانی پروتکل اینترنت بود. در سال ۱۹۹۵ میلادی نسخه جدید نشانی پروتکل اینترنت با نام IP نسخه ۶ معرفی گردید. اندازه آدرس از ۳۲ بیت به ۱۲۸ بیت افزایش یافت و امکان آدرس دهی تا ۲ به توان ۱۲۸ آدرس (یعنی خیلی آدرس : به عبارتی می گویند در هر متر مربع، ۱۰،۰۰۰ آدرس IP موجود خواهد بود) افزایش یافت. این کار تنها تعداد آدرس های اینترنتی را گسترش نداد، بلکه باعث خواهد شد جدول مسیریاب های اینترنتی (روتر ها) کوچکتر شود. کلیه سیستم عامل های جدید سرور و خانگی از جمله ویندوز ویستا به طور کامل پشتیبانی می شود ولی متاسفانه هنوز توسط بسیاری از مسیریاب های شبکه های خانگی و تجهیزات شبکه عادی پشتیبانی نشده است.

احتمالا در خیلی از مقاله ها و در سایت های مختلفِ تکنولوژی و فناوری، درباره آینده عجیبی که در آن همه وسایل اعم از PC، PDA گرفته تا تلفن سلولی (موبایل)، اتومبیل، یخچال و به طور کل لوازم خانگی که به اینترنت وصل می شوند، مطالبی را خوانده اید. برای مثال شما تصور کنید که از خانه خود برای انجام یک سفر به کشوری خارجی اعزام شده اید و شخصی در نبود شما بسته ای را برای شما می آورد و زنگ خانه شما را می زند در حالی که شما کیلومترها از خانه خود دور هستید و ناگهان تلفن همراه شما زنگ می خورد و دوربینی که در جلوی درب منزل خود نصب کرده اید تصویر شخص مورد نظر را بر روی تلفن همراه شما نمایان می سازد و مشاهده می کنید که بسته ای را برای شما آورده اند، از همان جا درب منزل خود را باز می کنید و با سیستم های صوتی به او می گویید که بسته را داخل منزل بگذارد و درب را بسته و قفل می نمایید و همه این کارها را به صورت از راه دور و به صورت Remote انجام می دهید.

خوب برای چند دقیقه رویای جالبی بود اما یک ایراد در این بین وجود دارد: هر دستگاهی که بخواهد به اینترنت متصل شود و معرفی شود بایستی آدرس IP خاص خود را داشته باشد. ولی برای این همه دستگاه الکترونیکی به اندازه کافی IP وجود ندارد. هیچ کس تصور نمی کرد که بیش از چهار میلیارد آدرس IP (که در IPv4.0 برای شناسایی تمامی کامپیوتر ها در نظر گرفته شده بود) یک روز تمام شود. اما امروزه خیلی ها پیش بینی می کنند که این آدرس ها حداکثر تا سال آینده بیشتر دوام نخواهد آورد.

اینترنت در دنیای غرب تقریباً همه جا را گرفته و با سرعتی که در آسیا و کشورهای توسعه یافته پیش می رود، همه آدرس های خالی در آینده پر خواهند شد. این که درصد بالایی از آدرس های IP به خاطر لجبازی و چشم و هم چشمی های دانشگاه ها و سازمان های آمریکایی حیف و میل شدند و IP های متعددی از پیش به آنها اختصاص داده شد فرقی در اصل قضیه نمی کند. مثلاً دانشگاه استنفورد بیش از ۱۷ میلیون آدرس IP را برای خود گرفته است و این در حالی است که کشوری همانند هند که بیش از یک میلیارد جمعیت دارد فقط ۲ میلیون آدرس IP را به خود اختصاص داده است.

امروزه بسیاری از شبکه های کامپیوتری با استفاده از NAT یا Network Address Translation آدرس های اینترنتی خود را افزایش داده و بدین روش کمبود خود را در داشتن آدرس های IP اختصاصی حل می کنند. NAT به روتر، فایروال و دیگر دستگاه ها این امکان را می دهد که یک آدرس IP جهانی را با سایر تجهیزات داخلی طوری به اشتراک بگذارد که هر کدام از دستگاه ها آدرس خصوصی مربوط به خود را داشته باشند. مسائل دیگری وجود دارند که نشان می دهد که عمر IPV4.0 (نسخه فعلی IP) رو به پایان است. برای مثال امروزه این توقع که ارتباط شما با اینترنت ضمن حرکت از ساختمانی به ساختمان دیگر، یا شهری به شهر دیگر و حتی کشوری به کشور دیگر پابرجا بماند خواسته ای بی جا به حساب نمی آید. در واقع تکنولوژی نسبتا جدیدی موسوم به IP Mobile برای تحقق بخشیدن به چنین خواسته هایی به وجود آمده است ولی این تکنولوژی با IPv4.0 به خوبی کار نمی کند و شامل نقص هایی است و همچنین قابل توجه است که این تکنولوژی بایستی توسط سیستمی پیاده سازی شود که دارای امنیت بالایی باشد ولی IPV4.0 از این مسئله تا حدودی فاصله دارد.

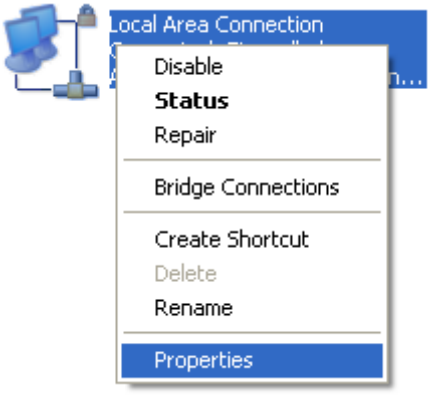
۲-۴-۱- در رابطه با IPv6.0 چه باید بدانیم؟

پروتکل جدید اینترنت که به نسل بعدی پروتکل اینترنت و یا IPNG که سر نام عبارت Internet Protocol Next Generation مشهور است، در سال ۱۹۹۵ به ستاد مهندسی اینترنت یا IETF پیشنهاد شد و پیش نویسی از آن در سال ۱۹۹۸ بـه تصـویب رسید. تکمیل این استاندارد و تعریف تمام بخش های آن نیز تا پاییز ۲۰۰۱ جزو دستور کار IETF بود. طی هفت سال گذشته IPV6.0 در انواع شبکه ها در بیش از ۴۰ کشور تحت آزمایش بوده است. در حال حاضر ژاپن آدرس های IPV6.0 را به مصرف کنندگان خود پیشنهاد می دهد. انتظار می رود که انتقال از IPV4.0 به IPV6.0 طی ده سال آینده یا شاید بیشـتر بـه انجـام برسد. برترین ویژگی IPV6.0 افزایش فضای آدرس دهی آن از ۳۲ بیت به ۱۲۸ بیت اسـت کـه مخـزن آدرس هـایIP را از ۴ میلیارد به ۳۵ تریلیون افزایش می دهد؛ و نکته جالب این جا است که با وجود چنین افزایشی، پردازش بسته هایIP پیچیـده تر نخواهد شد؛ چرا که در IPV6.0 فرمت هدر آدرس ها ساده تر شده است. به علاوه در IPV6.0 قابلیت اولویت دهی بر اساس محتوا نیز پیش بینی شده که نهایتا موجب بهبود کارایی و افزایش سرعت تحویل محتوا خواهـد شـد. از آنجـا کـه انتقـال بـه IPv6.0 نیازمند تغییرات در دستگاه ها و درایور ها و سیستم عامل ها است، لذا تردید در اجرای این استاندارد قابل قبول است. ولی طراحی IPv6.0 به صورتی انجام شده است که انتقال به آن طی یک فرایند تدریجی صورت بگیرد. در واقع زمان مشخصی برای انتقال کامل به این استاندارد وجود ندارد و شبکه ها می توانند سال هـا ترکیبـی از اسـتانداردهای IPV4.0 و IPV6.0 را مورد استفاده قرار بدهند. حال بهتر است بگوییم که نسل بعدی پروتکل اینترنت چه مزیت هایی نسبت به این پروتکـل فعلـی اینترنت دارد که قابلیت قرار گرفتن و همچنین دردسر برای راه انداختن آن را دارا است. قابلیت های این پروتکل جدید در زیر آمده است که عبارتند از:

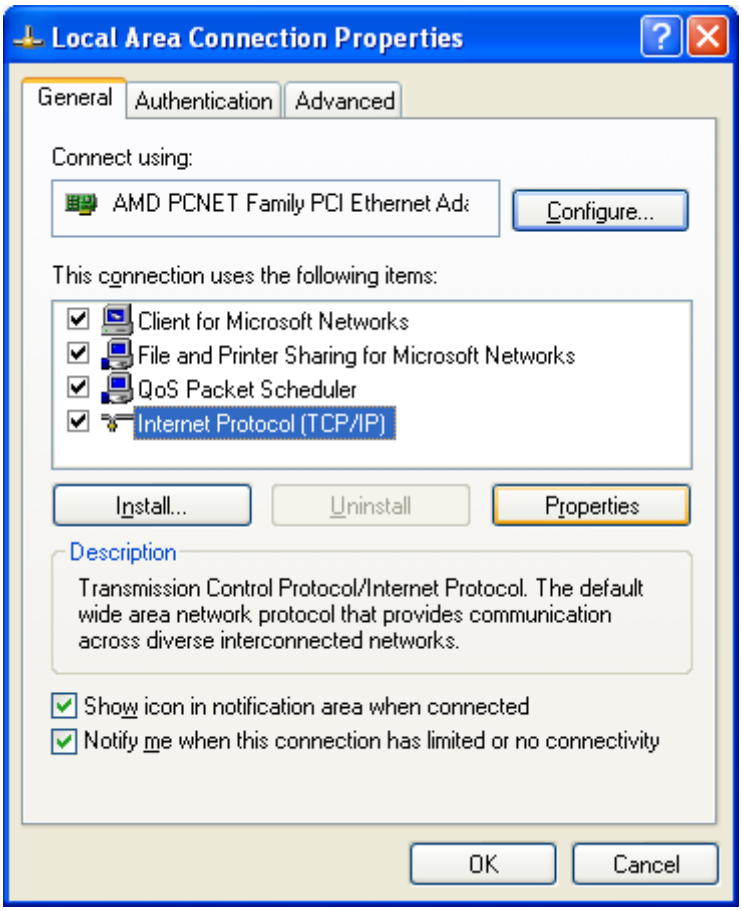
۱. فرمت سرآیند (Header) ساده تر شده است.
۲. اولویت دهی به بسته ها بر اساس محتوا
۳. پیکربندی خودکار (Auto Configuration)
۴. IP سیار (Mobile IP)
۵. امنیت (Security)
۶. کیفیت خدمات (Quality of Service)

۲-۵- تغییر آدرس IP در ویندوز XP

در این بخش به آموزش نحوه تغییر آدرس IP در ویندوز XP می پردازیم. بدین منظور پـس از اتصـال بـه شـبکه، وارد مسـیر Control Panel ➔ Network Connections می شویم. سپس روی Connection ساخته شده راست کلیـک کـرده و سـپس گزینه Properties را انتخاب می کنیم.

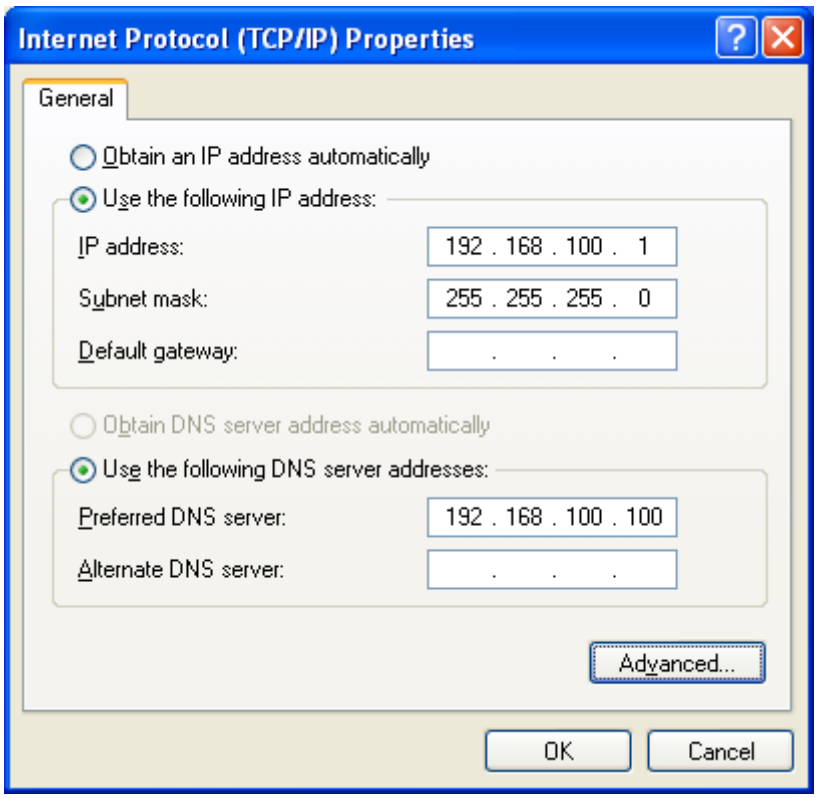


در صفحه باز شده، گزینه Internet Protocol (TCP/IP) را انتخاب نموده و سپس روی Properties کلیک نمایید.

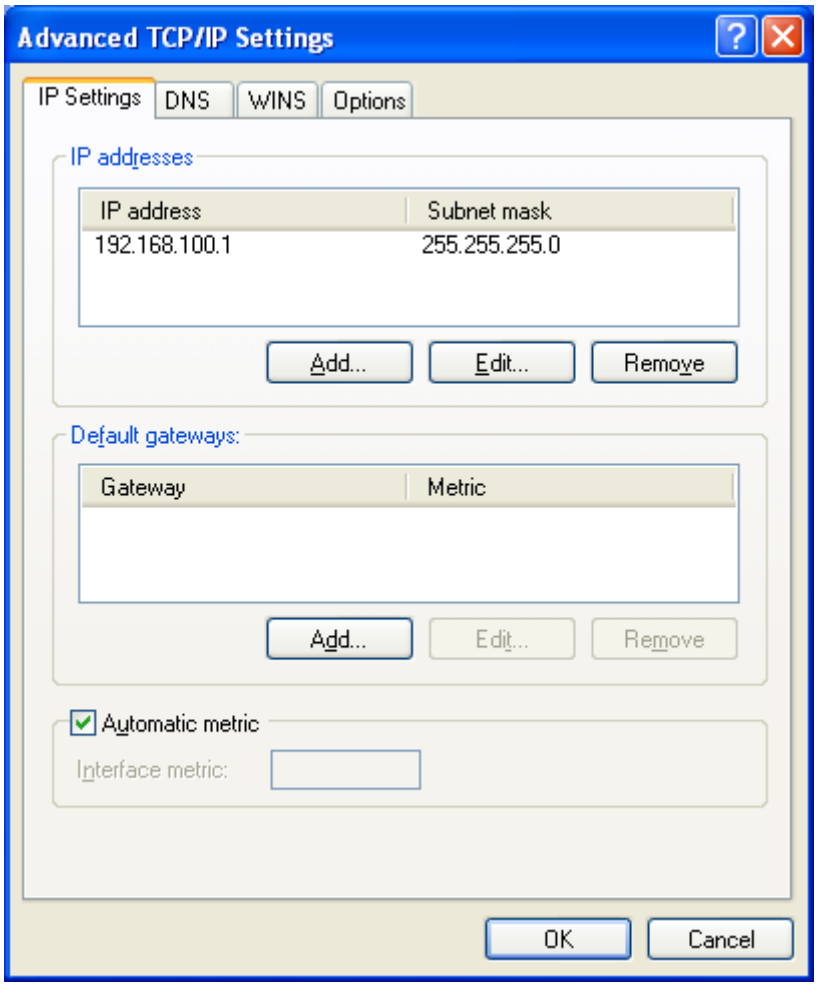


در صفحه باز شده، اگر می خواهید آدرس IP به صورت خودکار تعیین شده و کامپیوتر آدرس خود را از DHCP سرور بگیرد، گزینه **Obtain an IP address automatically** را انتخاب نمایید. اما اگر قصد دارید آدرس IP را دستی تعیین نمایید، گزینه **Use the following IP address** را انتخاب نمایید. سپس در قسمت **IP Address** آدرس IP را با توجه به نوع کلاس (A، B یا C) وارد نمایید. قسمت **Subnet Mask** با توجه به نوع آدرس IP تعیین می شود. ولی امکان تغییر آن نیز وجود دارد. در قسمت **Default Gateway** نیز دروازه پیش فرض که بسته های اطلاعاتی هنگام خروج از کامپیوتر به سمت آن می روند را تعیین نمایید. در قسمت **Preferred DNS server** نیز آدرس DNS Server که وظیفه تبدیل Host Name به IP Address عهده دارد را وارد نمایید. در قسمت **Alternate DNS server** نیز می توانید تعیین نمایید که اگر DNS Server اولیه جواب نداد، از یک DNS Server جایگزین استفاده نماید.

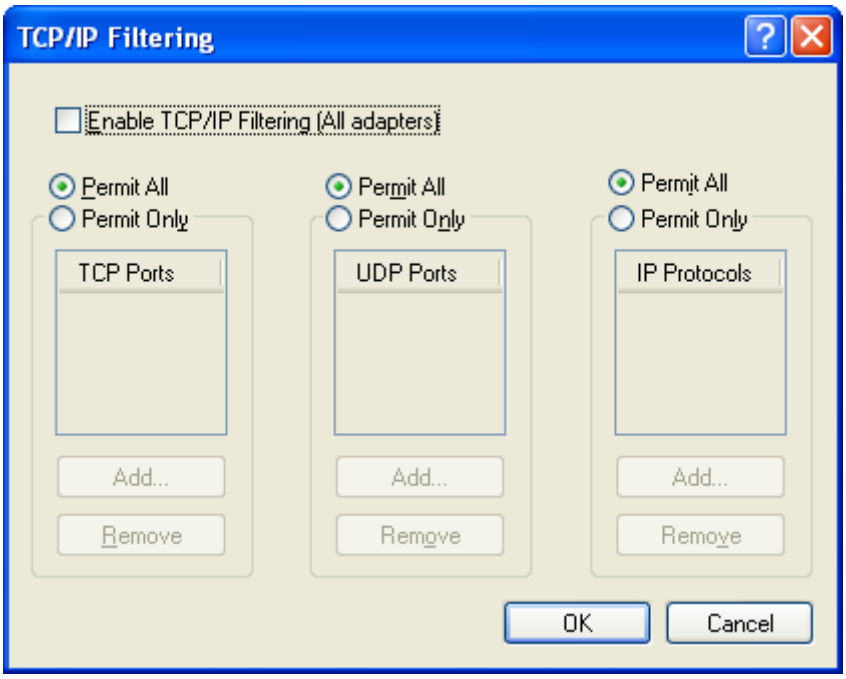
برای انجام تنظیمات پیشرفته تر، روی دکمه Advanced کلیک نمایید.



در صفحه باز شده امکان افزودن تنظیمات زیادتری وجود دارد. مثلاً در سربرگ IP Settings، می توان آدرس های IP یا دروازه های پیش فرض زیاد تری افزود. کامپیوتری که بیش از یک آدرس IP داشته باشد، به آن **Multi Home** می گویند. از طریـق سربرگ های DNS و WINS نیز می توان تنظیماتی را در مورد سرویس های DNS یا WINS انجام داد که این مفاهیم را در فصول بعدی توضیح خواهیم داد.

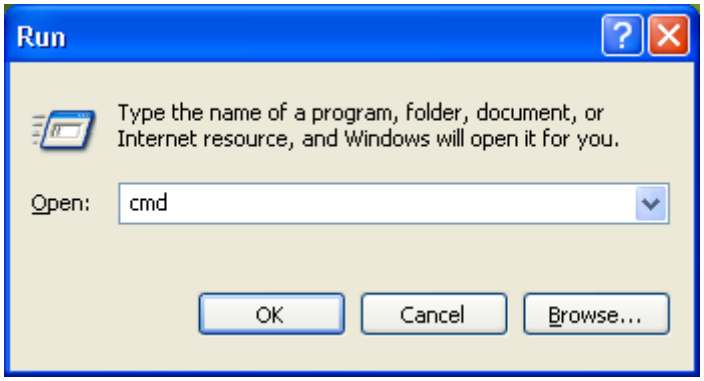


از طریق سربرگ Options نیز امکان مسدود کردن یا قابل اجرا کردن پورت های TCP یـا UDP خـاص یـا پروتکـل هـای IP وجود دارد. گزینه Permit All به معنای اجازه فعالیت به تمامی پورت ها وجود دارد. اما اگـر گزینـه Permit Only را انتخـاب نمایید، می توانید فعالیت پورت هایی خاص را توسط کلیک روی دکمه Add تعیین نمایید و بدین ترتیب دیگر پورت هایی که Add نشده اند، مسدود خواهند شد.



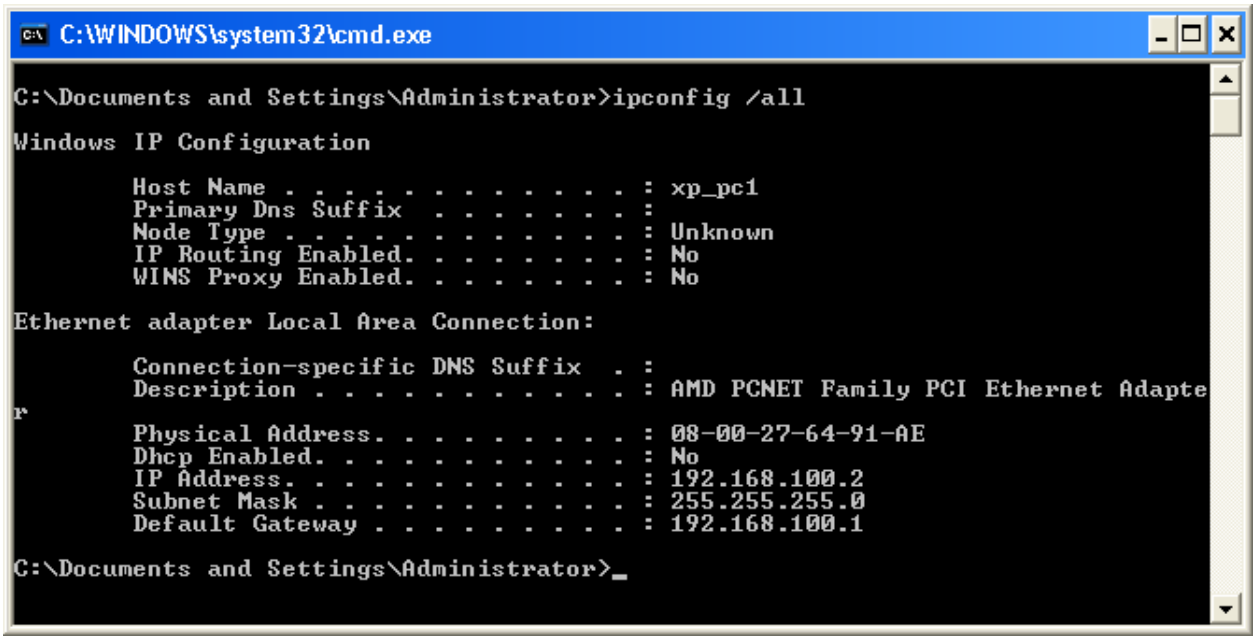
۲-۶- طریقه ی یافتن آدرس IP کامپیوتر

از منوی Start به گزینه Run می رویم و در آن تایپ می کنیم: cmd



سپس پنجره ای باز می شود. در آن پنجره تایپ می کنیم: ipconfig /all. بدین ترتیب می توانید بسیاری از تنظیمـات کـارت خود را مشاهده نمایید.

مشخصاتی ظاهر می شود که بیان گر کل مشخصات کارت های شبکه ی شما است. از میان اطلاعات ظـاهر شـده، ابتـدا پیـدا کنید که کدام کارت شما را به اینترنت متصل نموده، سپس در مقابل عبارت IP Address عددی را مشاهده خواهید کـرد کـه بیان گر IP ی شماست.



۲-۷- Subnet Mask چیست؟

هر IP Address توسط یک Subnet Mask از نظر تعداد بیت های Net ID و Host ID قابل تشخیص می گردد، و برای ماسک زدن به قسمتی از IP می توان استفاده نمود این ماسک تعیین می کند که کامپیوتر مقصد در شبکه Lan قرار گرفته یا یک شبکه راه دور. **در واقع Subnet Mask برای استخراج آدرس شبکه از داخل یک IP Address مورد استفاده قرار می گیرد.**

Subnet Mask در حالت Full Class یکی از سه حالت زیر است:

کلاس	مبنای ۱۰	مبنای ۲
Class A	۲۵۵.۰.۰.۰	۱۱۱۱۱۱۱۱.۰۰۰۰۰۰۰۰.۰۰۰۰۰۰۰۰.۰۰۰۰۰۰۰۰
Class B	۲۵۵.۲۵۵.۰.۰	۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۱۱.۰۰۰۰۰۰۰۰.۰۰۰۰۰۰۰۰
Class C	۲۵۵.۲۵۵.۲۵۵.۰	۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۱۱.۰۰۰۰۰۰۰۰

Subnet Mask در کلاس A به صورت ۲۵۵.۰.۰.۰ است. یعنی همان طور در بحث گذشته گفته شد، Net ID دارای هشت بیت است و بقیه بیت ها مربوط به Host ID می شوند.

Subnet Mask در کلاس B به صورت ۲۵۵.۲۵۵.۰.۰ است و در کلاس C به صورت ۲۵۵.۲۵۵.۲۵۵.۰ می باشد.

دقت داشته باشید که این Subnet Mask ها مربوط به سرویس دهنده ها هستند. به عنوان مثال Subnet Mask، با عدد ۲۵۵.۲۵۵.۲۵۵.۰ مربوط به سرویس دهنده ای (Server) است که از IP کلاس C برای سرویس دادن به مشتری هایش (Client) استفاده میکند. نه به ما که یک Host بر روی آن هستیم. Subnet Mask یک Client که روی IP کلاس C است ۲۵۵.۲۵۵.۲۵۵.۲۵۵ است، یعنی هیچ بیتی برای Host ندارد.

نحوه ساخت Subnet Mask، بدین صورت می باشد که در آدرس IP، به ازاء هر بیت Host ID، عدد ۱ و به ازاء هر بیت Net ID، عدد ۰ می گذاریم. سپس عدد به دست آمده را به مبنای ده می بریم. برای بردن به مبنای ده، عدد معادل هر کدام از چهار قسمت آدرس IP را جداگانه حساب می کنیم. برای مثال، کلاس A، ۸ بیت برای Net ID و ۲۴ بیت (۳ تا ۸ بیت) برای Host ID دارد. لذا داریم: ۱۱۱۱۱۱۱۱.۰۰۰۰۰۰۰۰.۰۰۰۰۰۰۰۰.۰۰۰۰۰۰۰۰ که معادل آن در مبنای ده برابر با عدد ۲۵۵.۰.۰.۰ می شود.

کاربرد Subnet Mask در ساخت کلاس های جدید شبکه است. فرض کنید که می خواهیم شبکه ای بسازیم که دارای 2^{12} شبکه و در هر شبکه دارای 2^{20} کامپیوتر باشد (۳۲=۱۲+۲۰ که آدرس IP ۳۲ بیتی است). لذا بایستی Subnet Mask را عوض کنیم. بدین منظور به تعداد بیت Net ID، عدد ۱ (در اینجا ۱۲ عدد) و به تعداد بیت Host ID، عدد ۰ (در اینجا ۲۰ عدد) می گذاریم. عدد به دست آمده در مبنای دو برابر ۱۱۱۱۱۱۱۱.۱۱۱۱۰۰۰۰.۰۰۰۰۰۰۰۰.۰۰۰۰۰۰۰۰ می باشد که معادل آن در مبنای ده می شود: ۲۵۵.۲۴۰.۰.۰. یعنی اگر Subnet Mask را به ۲۵۵.۲۴۰.۰.۰ تغییر دهیم، یعنی کلاس جدیدی در شبکه ساخته ایم که در این کلاس می توان 2^{12} شبکه و در هر شبکه می توان 2^{20} کامپیوتر داشت. البته بایستی به حالت خاص تمام بیت ها ۱ و تمام بیت ها ۰ نیز توجه نمود که باعث می شود از تعداد کل، دو عدد کمتر شود.

اگر Subnet Mask را دادند و تعداد شبکه و تعداد کامپیوتر در هر شبکه را خواستند، بایستی ابتدا، هر کدام از چهار قسمت Subnet Mask را جداگانه به مبنای ۲ برد (Subnet Mask نیز مانند IP Address، چهار قسمت دارد و در مجموع ۳۲ بیتی است). سپس تعداد شبکه برابر با $2^{\text{تعداد یک}}$ و تعداد کامپیوتر در هر شبکه برابر با $2^{\text{تعداد صفر}}$ می باشد.

اگر این مطلب را متوجه شده باشید به راحتی می توانید Subnet Mask را در بقیه کلاس ها و دیگر حالت ها به راحتی برای خود تحلیل کنید.

۲-۸- Default Gateway چیست؟

Default Gateway آدرسی (IP) است که نشان می دهد ما به کدام کامپیوتر متصل هستیم و از آن سرویس می گیریم. بنابراین در یک شبکه، تمام بسته های خارج شده از کامپیوتر، به سمت Default Gateway می رود و سپس Default Gateway در مورد آن بسته تصمیم گیری می کند. در مورد Default Gateway بعدا بیشتر صحبت خواهیم کرد.

۲-۹- Mac Address

مورد آخری که باقی می ماند این موضوع است، که با وجود اینکه مسیر یابی در شبکه بر اساس آدرس IP انجام می گیرد، اما سیستم ها قادر به تغییر آدرس IP خود هستند. با این وجود، شبکه از کجا تشخیص می دهد که هر آدرس IP مربوط به کدام کامپیوتر است؟ راه حل این است که هر کارت شبکه آدرسی سخت افزاری به نام Mac (Media Access Control) دارد که در تمام دنیا Unique (یکتا) است. آدرس سخت افزاری یا آدرس MAC، آدرس عددی است که به صورت سخت افزاری روی کارت واسط شبکه در کارخانه حک شده است. این نوع آدرس دهی موجب شناسایی منحصر به فرد کارت واسط شبکه در بین کارت ها می شود. طول این آدرس ۶ بایت است. استاندارد این آدرس دهی توسط انجمن مهندسان برق و الکترونیک (IEEE) تعیین شده است.

۲-۹-۱- دلیل استفاده از MAC Address

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

- **مدل OSI**

الف) Network Layer (لایه سوم): آدرس IP در این لایه قرار دارد.

ب) Data Link Layer (لایه دوم): آدرس MAC در این لایه قرار دارد.

ج) Physical Layer (لایه اول): شبکه فیزیکی

همانگونه که مشاهده می نمائید، MAC Address در لایه Data Link (لایه دوم مدل OSI) قرار دارد و این لایه مسئول بررسی این موضوع خواهد بود که داده متعلق به کدامیک از کامپیوتر های موجود در شبکه است. زمانی که یک بسته اطلاعاتی

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

۲-۹-۲- ساختار MAC Address

یک MAC Address بر روی هر کارت شبکه همواره دارای طولی مشابه و یکسان می باشند. (شش بایت و یا ۴۸ بیت). در صورت بررسی MAC Address یک کامپیوتر که بر روی آن کارت شبکه نصب شده است، آن را با فرمت مبنای شانزده (Hex)، مشاهده خواهید دید. مثلاً MAC Address کارت شبکه موجود بر روی یک کامپیوتر می تواند به صورت زیر باشد:

مشاهده MAC Address					
استفاده از دستور IPconfig /all و مشاهده بخش Physical address:					
A6	DB	79	BA	50	00
تعریف شده توسط تولید کننده			تعریف شده توسط IEEE با توجه به RFC 1700		

۲-۹-۳- مشاهده MAC Address

استفاده از دستور IPconfig /all در محیط Command Prompt و مشاهده بخش Physical address.

۲-۹-۴- قوانین تولید Mac Address

بر اساس قوانین تعریف شده توسط IEEE، زمانی که یک تولید کننده نظیر اینتل، کارت ها ی شبکه خود را تولید می نماید، آنان هر آدرس دلخواه ی را نمی توانند برای MAC Address در نظر بگیرند. در صورتی که تمامی تولید کنندگان کارت های شبکه بخواهند بدون وجود یک ضابطه خاص، اقدام به تعریف آدرس های فوق نمایند، قطعا امکان تعارض بین آدرس های فوق به وجود خواهد آمد. (عدم تشخیص تولید کننده کارت و وجود دو کارت شبکه از دو تولید کننده متفاوت با آدرس های یکسان). حتما این سوال برای شما مطرح می گردد که MAC Address توسط چه افراد و یا سازمان هایی و به چه صورت به کارت های شبکه نسبت داده می شود؟ به منظور برخورد با مشکلات فوق، گروه IEEE، هر MAC Address را به دو بخش مساوی تقسیم که از اولین بخش آن به منظور شناسائی تولید کننده کارت و دومین بخش به تولید کنندگان اختصاص داده شده تا آنان یک شماره سریال را در آن درج نمایند. با این که MAC Address در حافظه کارت شبکه ثبت می گردد، برخی از تولید کنندگان به شما این اجازه را خواهند داد که با دریافت و استفاده از یک برنامه خاص، بتوانید بخش دوم MAC Address کارت شبکه خود را تغییر دهید.

فصل ۳

انواع توپولوژی شبکه

۳-۱- توپولوژی شبکه

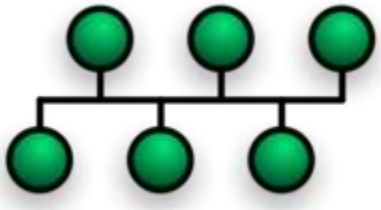
توپولوژی شبکه تشریح کننده نحوه اتصال کامپیوتر ها در یک شبکه به یکدیگر است. به عبارت دیگر، الگوی هندسی استفاده شده جهت اتصال کامپیوتر ها، توپولوژی نامیده می شود. پارامترهای اصلی در طراحی یک شبکه، **قابل اعتماد بودن** و **مقرون به صرفه بودن** است. توپولوژی انتخاب شده برای پیاده سازی شبکه ها، عاملی مهم در جهت **کشف و برطرف نمودن خطا** در شبکه خواهد بود. انتخاب یک توپولوژی خاص نمی تواند بدون ارتباط با محیط انتقال و روش های استفاده از خط مطرح گردد. نوع توپولوژی انتخابی جهت اتصال کامپیوتر ها به یکدیگر، مستقیماً بر نوع محیط انتقال و روش های استفاده از خط تاثیر می گذارد. با توجه به تاثیر مستقیم توپولوژی انتخابی در نوع کابل کشی و هزینه های مربوط به آن، می بایست با دقت و تامل به انتخاب توپولوژی یک شبکه همت گماشت. عوامل مختلفی جهت انتخاب یک توپولوژی بهینه مطرح می شود. مهمترین این عوامل بشرح ذیل است:

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

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

۳-۲- انواع همبندی (توپولوژی) شبکه

۳-۲-۱- آرایش خطی یا گذرگاهی (Bus)



شبکه ای که از همبندی گذرگاهی استفاده می کند معمولاً دارای یک کابل واحد (**معمولاً کابل Coaxial**) و بلند بوده که دستگاه های مختلف شبکه به آن متصل هستند (توسط T-Connector) و در هر واحد زمانی تنها یک رایانه امکان ارسال اطلاعات را دارد. در این روش کلیه رایانه های متصل به خط، اطلاعات ارسال شده را دریافت می کنند (**روش Broadcast**)؛ ولی تنها رایانه ای که آدرس مقصد بسته داده متعلق به او است این اطلاعات را ذخیره می نماید و بقیه رایانه ها از بسته صرف نظر می کنند. راه اندازی آن آسان است و به این منظور از یک رشته کابل کواکسیال استفاده می شود و هر سیستم به کمک یک **کانکتور** به شبکه متصل می شود. ابتدا و انتهای شبکه با **ترمیناتور** بسته می شود. اما نگهداری از آن با مشکلاتی همچون خطا یابی مشکل همراه است به همین دلیل تقریباً منسوخ شده است.

مزایای توپولوژی BUS

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

ساختار ساده. توپولوژی BUS دارای یک ساختار ساده است. در مدل فوق صرفاً از یک کابل برای انتقال اطلاعات استفاده می شود.

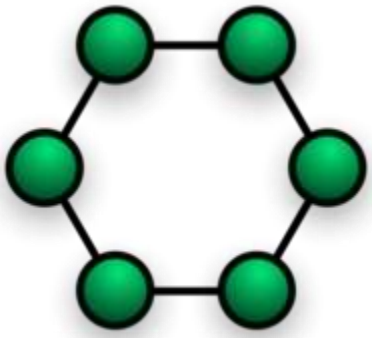
توسعه آسان. یک کامپیوتر جدید را می توان براحتی در نقطه ای از شبکه اضافه کرد. در صورت اضافه شدن ایستگاههای بیشتر در یک سگمنت، می توان از تقویت کننده هایی به نام Repeater استفاده کرد.

معایب توپولوژی BUS

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

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

۳-۲-۲- آرایش حلقوی (Ring)



این همبندی توسط شرکت IBM اختراع شد و کلیه رایانه ها به گونه ای به یکدیگر متصل هستند که مجموعه آنها یک حلقه را تشکیل می دهد. همیشه یک بسته کوچک با نام نشانه (Token) در داخل شبکه از یک رایانه به دیگری می رود، زمانی که یک رایانه اطلاعاتی جهت ارسال دارد، نشانه را در اختیار گرفته و از چرخش آن داخل شبکه جلوگیری می کند، تا زمانیکه نشانه توسط یک رایانه نگه داشته شده باشد، تمام رایانه های شبکه پذیرای اطلاعاتی خواهند بود که رایانه مالک نشانه ارسال می کند. که معایب این نوع توپولوژی این است که اگر قسمتی از کابل اصلی به علتی آسیب ببیند کل شبکه از کار می افتد و عیب یابی آن بسیار وقت گیر می باشد و از مزایای آن، می توان به **کم هزینه بودن و سادگی شبکه** اشاره کرد.

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

مزایای توپولوژی RING

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

نیاز به فضائی خاص جهت انشعابات در کابل کشی نخواهد بود. به دلیل استفاده از یک کابل جهت اتصال هر گره به گره همسایه اش، اختصاص محل هایی خاص به منظور کابل کشی ضرورتی نخواهد داشت.

مناسب جهت فیبر نوری. استفاده از فیبر نوری باعث بالا رفتن نرخ سرعت انتقال اطلاعات در شبکه است. چون در توپولوژی فوق ترافیک داده ها در یک جهت است، می توان از فیبر نوری به منظور محیط انتقال استفاده کرد. در صورت تمایل می توان در هر بخش از شبکه از یک نوع کابل به عنوان محیط انتقال استفاده کرد. مثلاً در محیط های اداری از مدل های مسی و در محیط کارخانه از مدل فیبر نوری استفاده کرد.

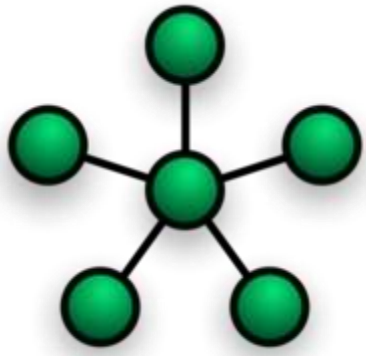
معایب توپولوژی RING

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

اشکال زدایی مشکل است. بروز اشکال در یک گره می تواند روی تمام گره های دیگر تاثیر گذار باشد. به منظور عیب یابی می بایست چندین گره بررسی تا گره مورد نظر پیدا گردد.

تغییر در ساختار شبکه مشکل است. در زمان گسترش و یا اصلاح حوزه جغرافیائی تحت پوشش شبکه، به دلیل ماهیت حلقوی شبکه مسائلی به وجود خواهد آمد.

۳-۲-۳- آرایش ستاره ای (Star)



در این نوع همبندی کلیه رایانه ها به یک کنترل کننده مرکزی به نام میانگاه (Hub) و یا سوئیچ (Switch) متصل می شوند و هرگاه رایانه ای بخواهد با رایانه دیگری تبادل اطلاعات کند رایانه مبدا اطلاعات را به میانگاه/سوییچ ارسال نموده و اطلاعات از طریق آن به رایانه مقصد انتقال می یابد.

نکته ها:

۱) یک پیوند **نقطه به نقطه** را می توان به عنوان حالت خاصی از یک شبکه با آرایش ستاره در نظر گرفت. در نتیجه ساده ترین شبکه که براساس آرایش ستاره ساخته می شود را می توان یک گره که به یک گره دیگر از طریق یک پیوند نقطه به نقطه متصل است در نظر گرفت انتخاب یک گره به عنوان میانگیر به دلخواه ممکن است.

۲) ساده ترین نوع شبکه براساس آرایش ستاره علاوه بر شبکه توضیح داده شده در فوق، یک میانگیر (Hub) متصل به دو گره می باشد.

۳) با وجود این که می توان آرایش ستاره را با استفاده از یک هاب (Hub) یا سوئیچ (Switch) براحتی پیاده سازی نمود، اما به کار بردن یک کامپیوتر یا یک اشتراک مشترک نیز برای میانگیر کافی است. به هر حال چون در بیشتر نمایش های آرایش ستاره یکی از این ابزار ویژه نشان داده شده است، در نتیجه ممکن است این ابهام به وجود آید که حتماً باید از یکی از این ابزار استفاده نمود در حالی که مثلاً سه کامپیوتر متصل به یکدیگر بدون استفاده از هیچ ابراز ویژه ای نیز خود یک شبکه با آرایش ستاره است.

۴) شبکه های ستاره را می توان به صورت پخشی (Broadcast) با دسترسی چندگانه (Multicast) یا غیر پخشی با دسترسی چندگانه (NBMA) توصیف نمود که وابسته به توانایی میانگیر در ارسال سیگنال های موجود به تمام گره های تابع یا ارسال سیگنال به صورت جداگانه برای هر ارتباط است.

مزایای توپولوژی STAR

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

در هر اتصال یک دستگاه. نقاط اتصالی در شبکه ذاتاً مستعد اشکال هستند. در توپولوژی STAR اشکال در یک اتصال، باعث خروج آن خط از شبکه و سرویس و اشکال زدایی خط مزبور است. عملیات فوق تاثیری در عملکرد سایر کامپیوتر های موجود در شبکه نخواهد گذاشت.

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

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

معایب توپولوژی STAR

زیاد بودن طول کابل. به دلیل اتصال مستقیم هر گره به نقطه مرکزی، مقدار زیادی کابل مصرف می شود. هزینه کابل نسبت به تمام شبکه، کم است، ام تراکم در کانال کشی جهت کابل ها و مسائل مربوط به نصب و پشتیبانی آن ها، به طور قابل توجهی هزینه ها را افزایش خواهد داد.

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

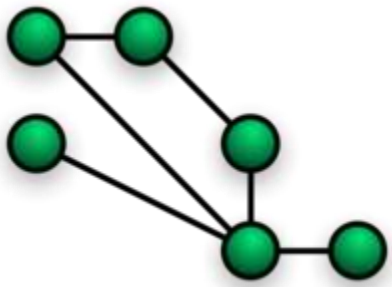
وابستگی به نقطه مرکزی. در صورتی که نقطه مرکزی (هاب یا سوئیچ) در شبکه با مشکل مواجه شود، تمام شبکه غیرقابل استفاده خواهد بود.

۳-۲-۴- ستاره گسترش یافته

اگر بین میانگیر (هاب یا سوئیچ) و گره ها (کامپیوتر ها)، تکرارکننده قرار دهیم تا مسافت قابل پوشش توسط میانگیر افزایش یابد، به آن آرایش **ستاره گسترش یافته** گفته می شود و اگر به جای تکرارکننده ها، میانگیر قرار داده شود، یک آرایش ترکیبی از ستاره سلسله مراتبی به وجود می آید که در بعضی از کتاب ها بین این آرایش و آرایش ستاره تفاوتی قائل نمی شوند.

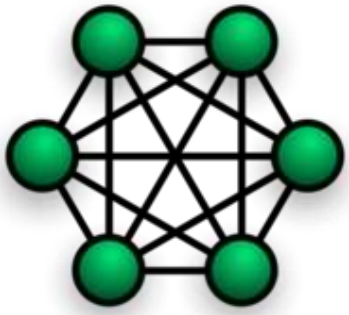
ماهیت تکرارکننده ها: در مواردیکه برای توسعه شبکه از تکرارکننده ها استفاده می گردد، ممکن است در ساختار شبکه تغییراتی نیز داده شود. موضوع فوق مستلزم بکارگیری کابل بیشتر و اضافه نمودن اتصالات مخصوص شبکه است.

۳-۲-۵- آرایش مشبک (Mesh)



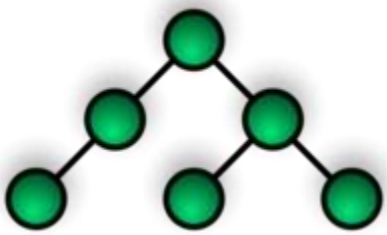
در این آرایش شبکه نظم مشخصی نداشته و هر یک از رایانه ها به یک یا چند رایانه دیگر متصل شده اند. این آرایش در واقع نسخه ناقص آرایش اتصال کامل است، لذا هزینه و پیچیدگی کمتری نسبت به روش مذکور دارد. از معایب این توپولوژی می توان به پیچیدگی و هزینه ی بالای آن اشاره کرد و چون شبکه گسترده است عیب یابی ان هم نسبت سخت می باشد. از مزایای این توپولوژی این است که اگر قسمتی از کابل قطع شود، کل شبکه از کار نمی افتد و انتقال اطلاعات به صورت دوبه دو می باشد؛ یعنی تمامی کامپیوتر ها بدون اینکه شبکه مشغول شود می توانند به یک دیگر اطلاعات ارسال و دریافت کنند که برای اینکه از توپولوژی Mesh بتوان از حداکثر استفاده را برد، از دستگاهی به نام روتر یا مسیر یاب استفاده می شود که کار این دستگاه این است که باعث می شود از خط ها یا مسیر هایی که خالی هستند ارسال اطلاعات انجام داد و در نتیجه این دستگاه باعث سرعت بخشیدن به ارسال اطلاعات می شود.

۳-۲-۶- آرایش اتصال کامل (Fully Connected)



در این آرایش تمام رایانه های شبکه مستقیماً به همدیگر متصل هستند. عمده ترین اشکال این روش پیچیدگی و هزینه بالای این اتصالات است. مزیت این روش ارسال سریع و بی واسطه اطلاعات از هر رایانه به رایانه دیگر می باشد. در این حالت اگر n کامپیوتر داشته باشیم، به $\frac{n\,(n-1)}{2}$ کابل نیاز خواهد بود.

۳-۲-۷- آرایش درختی (Tree) یا آرایش سلسله مراتبی



در آرایش درختی یک گره مرکزی (بالاترین سطح در سلسله مراتب) که ریشه نام دارد، 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 گره های سطح دو نیز به چندین گره در سطحی پایین تر متصل هستند (برای مثال در سطح سوم). گره مرکزی تنها گره ای است که هیچ گره ای در سطحی بالاتر از خود ندارد. سلسله مراتب درخت متقارن است یعنی تعداد گره های متصل به هر گره در سطح پایین تر عدد ثابت F است. عدد F به عنوان عامل شاخه بندی در درخت سلسله مراتب شناخته می شود.

نکته ها:

۱) یک شبکه مبتنی 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.

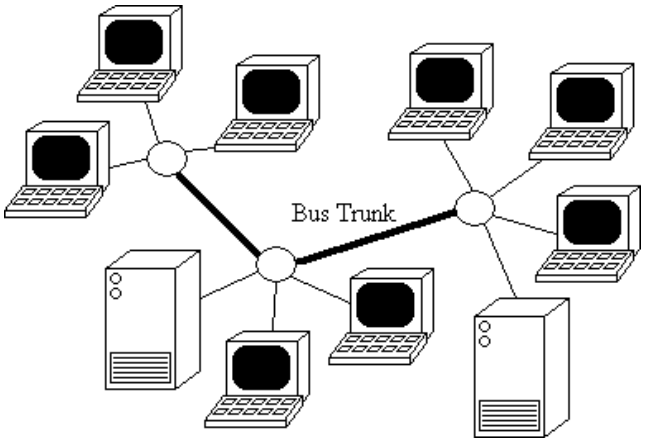
۲) اگر یک آرایش درختی عامل شاخه بندی برابر با یک داشته باشد این آرایش نشان دهنده آرایش خطی است.

۳) عامل شاخه بندی مستقل از تعداد کل گره ها است. اگر یک گره نیاز به درگاه هایی برای اتصال به گره های دیگر داشته باشد، می توان تعداد درگاه ها را بدون توجه به تعداد کل گره ها کاهش داد. در نتیجه تعداد درگاه های مورد نیاز وابسته به عامل شاخه بندی است و در نتیجه می توان تعداد درگاه ها را بدون توجه به تعداد کل گره ها کاهش داد.

۴) تعداد کل پیوندهای نقطه به نقطه در شبکه بر اساس آرایش درختی یکی کمتر از تعداد گره های شبکه می باشد.

۵) اگر نیاز به پردازش اطلاعات توسط گره ها در یک آرایش درختی فیزیکی باشد گره های سطح بالاتر باید پردازش بیشتری نسبت به گره های سطح پایین تر انجام دهند.

۳-۲-۸- آرایش ترکیبی (Hybrid)



آرایش ترکیبی نوعی از آرایش های شبکه است که از همبندی یک یا چند شبکه با آرایش های فیزیکی متفاوت و یا همبندی چندین شبکه که دارای آرایش فیزیکی یکسان است به وجود می آید و آرایش فیزیکی شبکه حاصل مشابه آرایش فیزیکی شبکه های اولیه نمی باشد (مثلاً آرایش فیزیکی شبکه ای که از همبندی چندین شبکه براساس آرایش فیزیکی ستاره بدست می آید ممکن است با توجه به نحوه اتصال شبکه ها به صورت ترکیبی از آرایش های ستاره و خطی یا ستاره و درختی باشد در حالی که اگر چندین شبکه با آرایش خطی توزیع شده به یکدیگر متصل گردند شبکه حاصل آرایش خطی توزیع شده را به خود خواهد گرفت)

این توپولوژی ترکیبی است از چند شبکه با توپولوژی متفاوت که توسط یک کابل اصلی بنام Backbone به یکدیگر مرتبط شده اند. توسط یک پل ارتباطی به نام Bridge به کابل Backbone متصل می شود.

فصل ۴

انواع ساختار شبکه

۴-۱- دسته بندی شبکه

شبکه های کامپیوتری از لحاظ منطقی به دو دسته تقسیم می شوند:

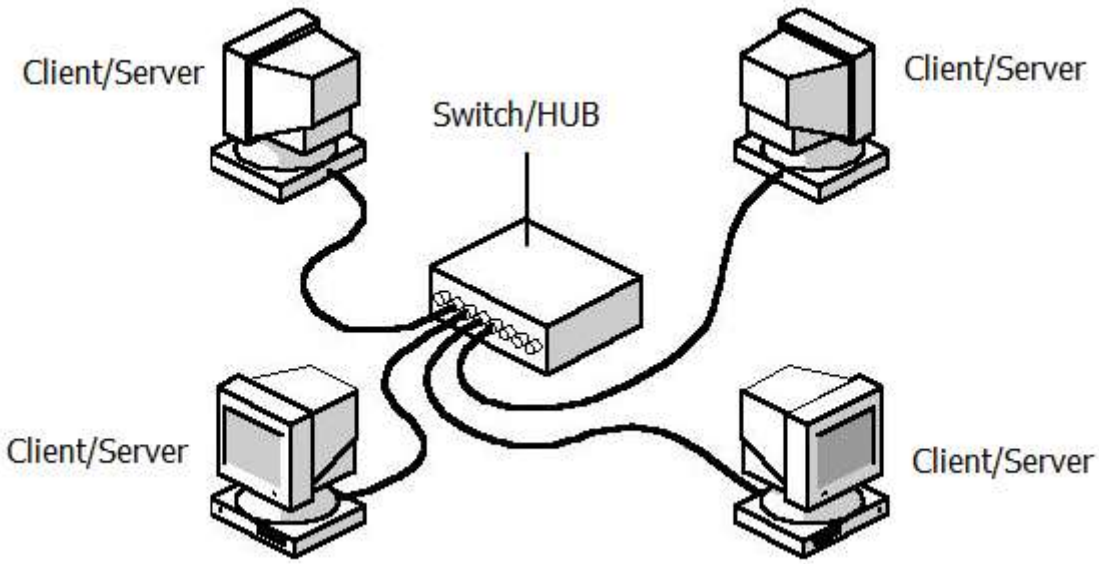
۱. **Work Group (Peer-To-Peer)**

۲. **Domain (Server Based یا Client - Server)**

در ادامه به معرفی هر کدام از روش های فوق خواهیم پرداخت:

۴-۲- Work Group (Peer-To-Peer)

شبکه های Peer-to-Peer : اگر در یک شبکه ای، سیستم ها همزمان علاوه بر ارایه ی سرویس، از سرویس های بقیه هم استفاده کنند یا به عبارتی به طور همزمان هم سرویس دهنده باشند و هم سرویس گیرنده، در این صورت می گوییم مدل سرویس دهی در شبکه به صورت Peer-to-Peer یا نظیر به نظیر است. (به اختصار PtP).



۴-۲-۱- معرفی مدل Peer-To-Peer (نظیر به نظیر)

در شبکه های نظیر به نظیر، سرویس دهنده اختصاصی وجود نداشته و سلسله مراتبی در رابطه با کامپیوتر ها رعایت نمی گردد. تمام کامپیوتر ها معادل و همتراز می باشند. هر کامپیوتر در شبکه هم به عنوان سرویس گیرنده وهم به عنوان سرویس دهنده ایفای وظیفه نموده و امنیت به صورت محلی و بر روی هر کامپیوتر ارائه می گردد.(هر کامپیوتری مسئول تعیین امنیت

و سیاست های کاری خود می باشد). کاربر هر یک از کامپیوتر ها مشخص می نماید که چه داده ای بر روی کامپیوتر خود را به اشتراک قرار دهد. شبکه های نظیر به نظیر، Workgroup نیز نامیده می شوند. واژه Workgroup، نشان دهنده یک گروه کوچک (معمولاً ۱۰ و یا کمتر) از کامپیوتر های مرتبط با یکدیگر است. شبکه های نظیر به نظیر، گزینه ای مناسب برای محیط هایی با شرایط زیر می باشند:

۱. حداکثر تعداد کاربران ۱۰ و یا کمتر.
۲. کاربران منابع و چاپگرها را به اشتراک گذاشته و در این راستا، سرویس دهندگان خاصی وجود ندارد.
۳. امنیت متمرکز مورد نظر نباشد.
۴. رشد سازمان و شبکه بر اساس آنالیز شده، محدود باشد.
۵. این نوع شبکه ساده ترین و سریعترین روش شبکه سازی به ویژه در محیط های ویندوز می باشد که ابزار خاصی لازم نداشته و دارای مزایای زیر می باشد:
۶. هزینه راه اندازی و نگهداری پایین تر
۷. سرعت بیشتر در راه اندازی
۸. عدم نیاز به یک کامپیوتر مجزا به عنوان سرور

۴-۲-۲- شبکه سازی به روش نظیر به نظیر

برای ایجاد چنین شبکه ای تجهیزات زیر لازم است:

۱. کارت شبکه.
۲. کابل شبکه.
۳. سوکت از نوع استاندارد RJ45 که به سر کابل ها وصل می شود.
۴. میانگاه (Hub) یا سوئیچ (Switch) در صورتی که بیش از دو رایانه را بخواهید شبکه کنید.
۵. نرم افزار مناسب: به عنوان مثال سیستم عامل ویندوز به تنهایی می تواند کافی باشد.
۶. برخلاف حالت Client/Server در این روش کامپیوتر های شخصی می توانند بدون Server به هم متصل شده و تبادل اطلاعات نمایند. پس از نصب مراحل سخت افزاری فقط کافی است که سرویسهای شبکه را در ویندوز و یا سیستم عامل های دیگر همچون لینوکس نصب کرده و دیسک گردان ها (درایو ها) را به اشتراک گذارید.
۷. ادعا می شود که امنیت آن از روش Client/Server بالاتر است. (اما نقیض این صحبت را جلوتر اعلام خواهیم کرد)
۸. نیاز به Administrator (مدیر شبکه) ندارد.

یکی از کاربردهای شبکه نظیر به نظیر دسترسی یافتن از طریق رایانه شخصی خود به پرونده هایی است که در سخت دیسک رایانه دیگری قرار دارد.

به طور پیش فرض شبکه ها در ویندوز به صورت Workgroup هستند. برای مشاهده این قسمت ابتدا بر روی My Computer راست کلیک کرده و گزینه ی Properties را انتخاب کنید. سپس Tab دوم یعنی Computer Name را انتخاب کنید. در این قسمت می توانید با کلیک بر روی گزینه یChange تنظیمات را مشاهده کنید. در فیلد آخر که Workgroup است، می توانید یک نام دیگر برای گروهتان در نظر بگیرید و بدین صورت کامپیوتر های موجود در شبکه را دسته بندی کنید. مثلاً ۵ کامپیوتر در گروه IT و ۵ کامپیوتر در گروه Computer. این نکته بسیار مهم است که قرار گرفتن کامپیوتر ها در دسته های گوناگون، باعث مسدود شدن دسترسی به منابع آنها نمی شود. در واقع ۲ کامپیوتر می توانند عضو دو گروه کاری متفاوت باشند اما در عین حال منابع یکدیگر را ببینند و در صورت لزوم ویرایش کنند. تنها فایده ی این دسته بندی ها، راحتی کار در هنگام در هنگام جست و جو است. به همین دلیل این نوع شبکه ها، جز شبکه هایی با امنیت پایین (Low Security) هستند. (نقیض ادعایی که در بالا مطرح شد.)

حال سوالی که مطرح می شود این است که آیا هر کامپیوتری با وصل کردن کابل شبکه می تواند وارد این چرخه شود و از منابع بقیه کامپیوتر ها استفاده کند؟

جواب منفی است. درست است گفتیم این شبکه ها **Low Security** هستند اما نه آنقدر. هر کامپیوتر بخشی به نام **LSD** (**L**ocal **S**ecurity **D**atabase) دارد که اطلاعات مربوط به کاربران را در خود ثبت می کند. LSD هر کامپیوتر نیز متعلق به خود آن کامپیوتر است. این قسمت از طریق راست کلیک کردن بر روی My Computer و انتخاب Manage و سپس Local Users and Groups قابل دسترسی است. در شبکه های Workgroup برای اتصال به کامپیوتر دیگر، باید یک User و Pass وارد کرد که این دو، همان نام کاربری و رمز عبور شما در ویندوز هستند. بعد از وارد کردن این اطلاعات، کامپیوتر میزبان در LSD خود به دنبال این اطلاعات می گردد و اگر User Name و Password شما در LSD آن موجود بود، به شما اجازه ی دسترسی می دهد.

نکته ای که اینجا وجود دارد این است که اگر شما در کامپیوتر خود دارای حساب Admin هستید اما در کامپیوتر دیگر به عنوان یک کاربر معمولی تعریف شده اید، در هنگام اتصال به آن کامپیوتر شما تنها اجازه ی دسترسی در حد یک کاربر معمولی را دارید. بنابراین در شبکه های Workgroup چیزی که اهمیت دارد کامپیوتر میزبان است و نه کامپیوتر میهمان.

۴-۲-۳- ویژگی ها

به نظر میرسد تنها ویژگی این نوع شبکه ها نصب و راه اندازی فوق آسان و همچنین هزینه ی کم باشد.

۴-۲-۴- معایب

۱. **Low Security**: در قسمت قبل چرایی پایین بودن امنیت این شبکه ها را باهم بررسی کردیم.
۲. **No Centralize Manage**: در این نوع شبکه ها، هیچ گونه مدیریت مرکزی وجود ندارد. به عنوان مثال در صورت اضافه شدن یک کاربر جدید، باید User و Pass آن را، در **LSD** همه ی کامپیوتر ها به صورت دستی وارد کرد و این یعنی فاجعه!
۳. **Limit 10**: تعداد کاربران در این نوع شبکه ها محدود است و بهترین حالت آن تا ۱۰ کاربر است. برای توضیح علت این موضوع باید کمی از بحث خارج شویم:

ما در شبکه ها ۳ نوع ارسال Packet داریم:

- **Uni Cast**: اگر آدرس مقصد Packet (داده ارسالی)، یکی باشد، نوع ارسال **Uni Cast** است.
- **Multi Cast**: اگر آدرس مقصد Packet، چند تا باشد، نوع ارسال **Multi Cast** است. در این روش فقط کامپیوتر هایی Packet را دریافت می کنند که Packet به سمت آن ها ارسال شده باشد.
- **Broad Cast**: اگر آدرس مقصد Packet، یک دسته باشد، نوع ارسال **Broad Cast** است. در این روش تمام کامپیوتر ها Packet را دریافت می کنند، اما فقط کامپیوتر هایی از Packet استفاده می کنند که آدرس آن ها در Packet قید شده باشد.

این نکته را هم داشته باشید که در شبکه ها، هیچ گاه در حالت عادی نمی توان از طریق نام یک کامپیوتر به آن کامپیوتر ها دسترسی پیدا کرد (نیاز به تبدیل نام کامپیوتر به آدرس IP وجود دارد).

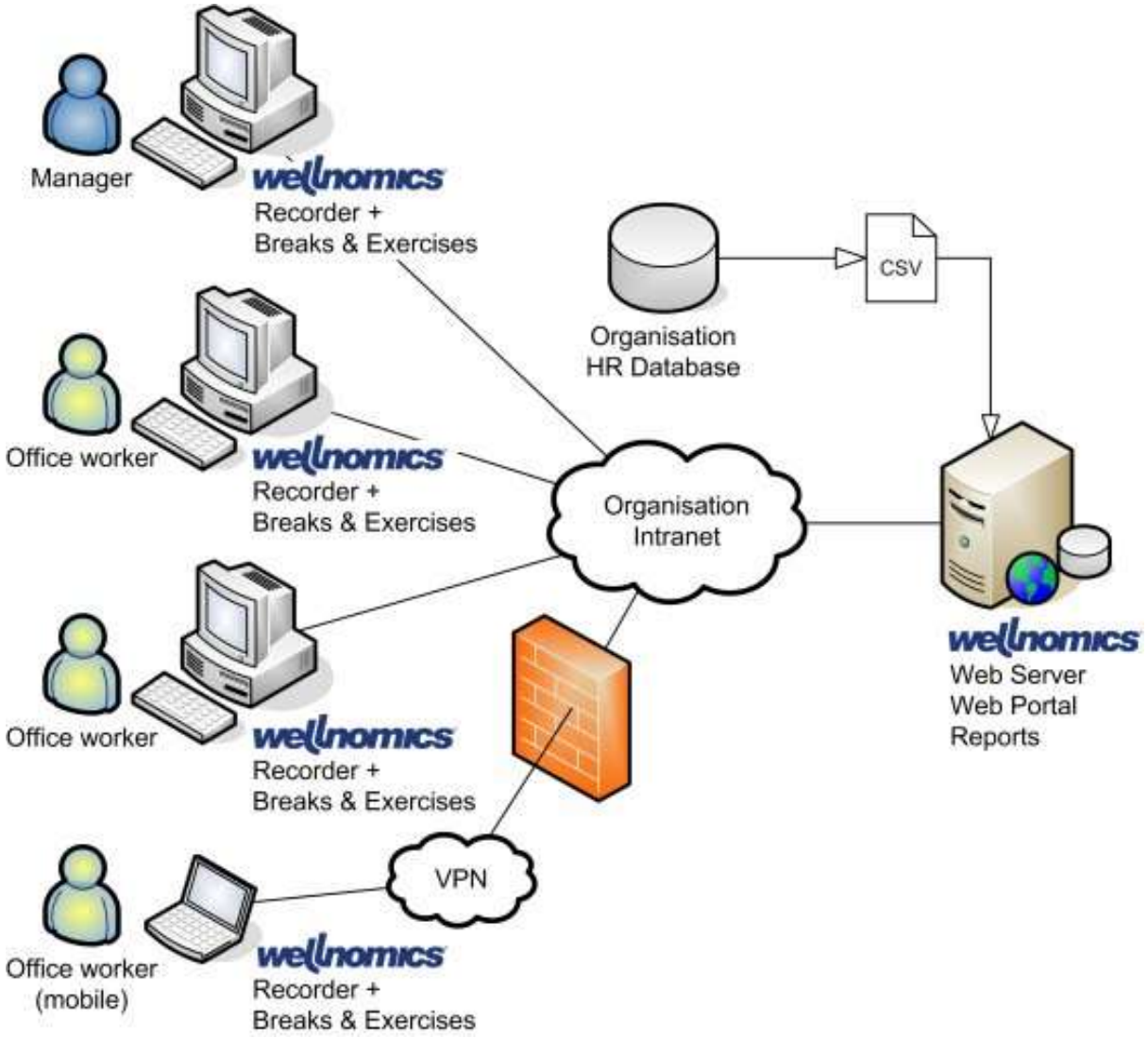
قضیه خیلی ساده شد. چون در شبکه های Work Group هیچ سرویسی برای تبدیل IP به اسم و بر عکس وجود ندارد، بنابراین برای اتصال به یک کامپیوتر، یک Packet به صورت Broad Cast به همه ی کامپیوتر ها ارسال می شود تا کامپیوتر مورد نظر شناسایی شود. به همین دلیل است که با افزایش تعداد کاربران، سرعت این نوع شبکه به شدت افت پیدا می کند.

۴-۳- دامنه یا Domain در Server Based یا Client - Server

اگر در یک شبکه تعدادی از سیستم ها فقط در نقش سرویس دهنده و تعدادی فقط در نقش سرویس گیرنده ظاهر شوند در این صورت می گوییم که مدل سرویس دهی آن شبکه به صورت Server –Based (به اختصار SB) است.

۴-۳-۱- معرفی شبکه های Server Based یا Client-Server

به موازات رشد شبکه و افزایش کاربران و منابع موجود، یک شبکه نظیر به نظیر قادر به پاسخگوئی به حجم بالای تقاضا برای منابع اشتراکی نخواهد بود. به منظور هماهنگی با افزایش تقاضا و ارائه سرویس های مورد نیاز، شبکه ها می بایست از سرویس دهندگان اختصاصی استفاده نمایند. یک سرویس دهنده اختصاصی، صرفاً به عنوان یک سرویس دهنده در شبکه ایفای وظیفه می نماید (نه به عنوان یک سرویس گیرنده). شبکه های سرویس گیرنده - سرویس دهنده، به عنوان مدلی استاندارد برای برپاسازی شبکه مطرح شده اند. به موازات رشد یک شبکه (تعداد کامپیوتر ها متصل شده، فاصله فیزیکی، ترافیک موجود) می توان تعداد سرویس دهندگان در شبکه را افزایش داد. با توزیع مناسب فعالیت های شبکه بین چندین سرویس دهنده، کارآیی شبکه به طرز محسوسی افزایش خواهد یافت.



سرویس دهی در این شبکه توسط سیستم هایی صورت می گیرد که اصطلاحا سرویس دهنده یا Sever نامیده می شوند. سیستم هایی که از این سرویس استفاده می کنند اصطلاحا سرویس گیرنده یا Client نامیده می شوند. برای سرویس گیرنده ها اصطلاح Workstation نیز به کار می رود.

۴-۴- تعاریف دیگری برای Client و Server

Server یا سِرور به برنامه ای رایانه ای گفته می شود که خدمات خود را به دیگر برنامه های رایانه ای (و کاربران آن ها) در همان رایانه یا در رایانه های دیگر ارائه می کند. به رایانه ای که چنین برنامه ای روی آن اجرا شود نیز Server گفته می شود. Serverها انواع گوناگونی دارند، نظیر: Application Server, Web Server, Backup Server

Client، یک نرم افزار کاربردی یا سامانه ای است که به خدمات یک سامانه رایانه ای دیگر به نام Server از طریق یک شبکه دسترسی دارد.

این عبارت نخستین بار برای نرم افزارهایی که قابلیت اجرای برنامه های مستقل خودشان را نداشتند اما می توانستند با رایانه های دور از طریق شبکه برهم کنش داشته باشند، به کار رفت. مدل Client-Server امروزه نیز در اینترنت به کار می رود. مرورگر های وب، Client هایی هستند که به Serverهای وب وصل می شوند و صفحات وب را برای نمایش بازیابی می کنند.

یک مدل Client-Server، یک ساختار توزیع شده است که وظایف یا حجم کار را بین سرویس دهنده ها و سرویس گیرنده ها تقسیم می کند.

یک معماری Client-Server یک معماری شبکه ای است که در آن هر رایانه یا پردازش روی شبکه یا یک Server است، یا یک Server. Clientها معمولاً رایانه های پرقدرت، یا پردازش هایی هستند که مختص انجام کار خاصی مانند مدیریت دیسک گردان ها، چاپگر ها، مدیریت ترافیک شبکه می باشند.

Clientها، ایستگاه های کاری یا رایانه های شخصی هستند که کاربران بر روی آن ها برنامه های کاربردی را اجرا می نمایند.Client ها به منابعی که Server به آنها اختصاص می دهد مانند، پرونده، دستگاه ها، و قدرت پردازش اعتماد دارند. این معماری از سایر معماری ها در این نکته متمایز است که می تواند با استفاده از لایه ها ساختار دهی مطمئنی از سیستم به وجود آورد.

در سال های اخیر استفاده از یک Client کوچک (Thin Client) که حاوی منطق کاری نیست، و تنها عناصر رابط کاربری جهت اتصال به یک Server کاربردی که منطق کاری روی آن پیاده سازی شده باب شده است.

تنها نکته ای که در مورد Server Based بسیار حائز اهمیت می باشد، این است که Serverها مدیریت کل شبکه را بر عهده دارند و Clientها فقط کارهایی را می توانند انجام دهند که Server اجازه انجام آن کارها را به Clientها داده باشد. (و این یعنی مدیریت متمرکز). مثلاً کاربری مانند Ali، فقط اجازه دارد که از کامپیوتر های خاصی استفاده کند یا مثلاً حق دارد ماهیانه فقط ۱۰۰ عدد چاپ و آن هم با چاپگری خاص بگیرد.

فصل ۵

سیستم عامل شبکه

۵-۱- سیستم های عامل شبکه ای

هسته یک شبکه، سیستم عامل شبکه (Network Operating System) است. همانگونه که یک کامپیوتر بدون استفاده از سیستم عامل، قادر به انجام عملیات خود نخواهد بود، یک شبکه (چه شبکه Workgroup و چه شبکه Server Based) نیز بدون وجود یک سیستم عامل شبکه ای، قادر به انجام عملیات و ارائه سرویس های مربوطه نخواهد بود.

به عبارت دیگر، سیستم عامل شبکه، سیستم عاملی است که ویژه پشتیبانی از شبکه طراحی می شود. همین طور می توان گفت سیستم عامل شبکه، نرم افزاری است که یک شبکه و **ترافیک و صف پیام های روی آن** را کنترل می کند. همچنین **کنترل دسترسی چندین کاربر به یک منبع** بر روی شبکه نظیر یک فایل را بر عهده دارد و عملیات مدیریتی مهمی نظیر **کنترل امنیت** را میسر می سازد. سیستم عامل های مبتنی بر سرویس دهنده (Server) علاوه بر کارهای **نظارتی، امنیتی و مدیریتی**، پشتیبانی از کار در شبکه را نیز هم زمان برای چندین کاربر فراهم می کنند. سیستم عاملی که از وجود شبکه آگاه باشد (Network-Aware) می تواند امکان دستیابی به منابع شبکه را برای کاربران فراهم سازد. بر خلاف سیستم عامل های تک کاربره، این سیستم عامل ها باید درخواست های دریافتی از ایستگاه های کاری مختلف را پاسخ گویند و جزئیاتی چون دستیابی و ارتباطات شبکه، تخصیص و به اشتراک گذاشتن منابع، محافظت داده ها و کنترل خطاها را نیز مدیریت کنند. سر نام سیستم عامل های شبکه، NOS است که Network OS نیز نامیده می شود.

سیستم های عامل شبکه ای، سرویس ها و خدمات خاصی را در اختیار کامپیوتر های موجود در شبکه قرار خواهند داد:

۱. هماهنگی لازم در خصوص عملکرد دستگاه های متفاوت در شبکه به منظور حصول اطمینان از برقراری ارتباط در مواقع ضروری
۲. امکان دستیابی سرویس گیرندگان به منابع شبکه نظیر فایل ها و دستگاه های جانبی نظیر چاپگر ها و دستگاه های فاکس
۳. اطمینان از ایمن بودن داده ها و دستگاههای موجود در شبکه از طریق تمرکز ابزارهای مدیریتی

۵-۲- ویژگی های یک سیستم عامل شبکه ای

یک سیستم عامل شبکه ای می بایست امکانات و خدمات اولیه زیر را ارائه نماید:

۱. ارائه مکانیزم های لازم به منظور برقراری ارتباط بین چندین دستگاه کامپیوتر برای انجام یک فعالیت خاص
۲. حمایت از چندین پردازنده

۳. حمایت از مجموعه ای (کلاستر) دیسک درایو – پردازنده - حافظه
۴. ارائه امکانات و سرویس های امنیتی در رابطه با حفاظت از داده ها و سایر منابع موجود در شبکه
۵. قابلیت اطمینان بالا
۶. تشخیص و برطرف نمودن خطا با سرعت مناسب

بر اساس نوع سیستم عامل، یک نرم افزار شبکه ای می تواند به سیستم عامل، اضافه و یا به صورت یکپارچه با سیستم عامل همراه باشد. نرم افزار سیستم عامل شبکه ای با مجموعه ای از سیستم های عامل رایج نظیر: ویندوز سرور (۲۰۰۰، ۲۰۰۳ و ۲۰۰۸)، ویندوز NT، ویندوز ۹۸، ویندوز ۹۵، و اپل مکینتاش، به صورت یکپارچه همراه می گردد.

البته نکته ای دیگر وجود دارد و آن اینکه برای راه اندازی یک شبکه، همیشه نیاز به داشتن سیستم عامل شبکه وجود ندارد. بلکه می توان از سیستم عامل های همه منظوره (مثل Windows XP) استفاده کرد. به خصوص در شبکه های Workgroup این موضوع بسیار مطرح می شود. اما اگر بخواهیم شبکه ای به مفهوم واقعی راه اندازی کنیم (Server Based)، عقل سلیم می گوید که برای Server از یک سیستم عامل شبکه استفاده کنیم.

برخی از سیستم عامل های معروف شبکه به قرار زیر است:

- Windows NT
- IBM AIX
- Sun Solaris
- Plan 9 from Bell Labs
- Inferno
- Windows 2000, 2003, 2008 Server
- Novell NetWare
- Linux (Red Hat, Ubuntu, SUSE, …)
- Unix… ,

۵-۳- معرفی انواع سرور

۵-۳-۱- *File Server*

یک سروری می باشد که از طریق آن می توان امکانی جهت مدیریت فایل ها و دسترسی کاربران مختلف شبکه در درایو های مختلف به صورت متمرکز بر روی یک سرور در شبکه خود برقرار کنیم؛ که جهت راه اندازی این نوع سرور در Windows Server از طریق Manage Your Server option در منوی Administrative Tools اقدام می کنیم.

۵-۳-۲- *Print Server*

اگر بر روی کامپیوتری ویندوز سرور نصب شود و این کامپیوتر مجهز به یک دستگاه چاپگر باشد و این چاپگر جهت دسترسی کاربران مختلف شبکه به اشتراک گذاشته شود (Share)، این کامپیوتر می تواند به عنوان Print Server مورد استفاده قرار گیرد.

۵-۳-۳- *Application Server*

سروری می باشد که بر روی آن برنامه های تحت وب قرار می گیرد و از طریق سرویس IIS (Internet Information Services) این برنامه در اختیار کامپیوتر های دیگر شبکه قرار می گیرد.

تعریف دیگری نیز وجود دارد و آن اینکه رایانه ای است که نرم افزارهای کاربردی را به درخواست کاربران برای آنها اجرا کرده و نتایج حاصل از اجرا را روی رایانه خودشان نمایش می دهد. هسته ی مرکزی روی سرویس دهنده است و نه سرویس گیرنده. در اینجا سرویس گیرنده تنها یک درخواست کننده برای اجرای عمل است.

دلایل استفاده از Application Server:

- امکانات سخت افزاری سرویس گیرنده ممکن است برای اجرای مستقیم برنامه کافی نباشد، مانند دستگاههای ATM
- نیاز به مدیریت بیشتر و کنترل نرم افزار ها

۵-۳-۴- Terminal Server

توسط این سرویس می توان به صورت Remote یا از راه دور به سرور متصل شده و به مدیریت مربوطه را انجام دهیم و یا برنامه ای تحت شبکه را بدین طریق و با استفاده از این سرویس اجرا نمود.

۵-۳-۵- VPN Server / Remote Server

توسط این سرور ها می توانیم به کاربران مختلف جهت متصل شدن به صورت راه دور (Remote) به شبکه داخلی مجوز هایی را بدهیم و یا با استفاده از VPN (Virtual Private Network) ارتباطی امن بین دو نقطه ایجاد کنیم. (با کمک پروتکل های PPTP، L2TP، SSTP و ...)

۵-۳-۶- DNS Server

سروری می باشد که کار Name Resolution را برای ما انجام می دهد و وظیفه آن تبدیل IP به اسم و بالعکس می باشد.

۵-۳-۷- DHCP Server

DHCP مخفف Dynamic Host Configuration Protocol می باشد. این سرور از طریق محدوده IP که بر روی آن تعریف می شود به صورت اتوماتیک به کلاینت ها IP می دهد و بسیاری کار های دیگر که به جای خود به آن اشاره خواهیم کرد. در ضمن این سرویس حتما باید بر روی کامپیوتری که نسخه سرور دارد نصب شود.

۵-۴- ویندوز سرور ۲۰۰۳

سیستم عامل ویندوز سرور ۲۰۰۳، امکانات گسترده و پیشرفته ای را در اختیار کاربران قرار می دهد:

- **Multitasking**: با استفاده از ویژگی فوق، کاربران قادر به اجرای چندین برنامه به صورت همزمان بر روی یک سیستم می شوند. تعداد برنامه هایی که یک کاربر قادر به اجرای همزمان آنان خواهد بود به میزان حافظه موجود بر روی سیستم بستگی خواهد داشت.
- **Memory Support**: به منظور انجام عملیات مربوط به برنامه هایی که در محیط ویندوز ۲۰۰۳ اجراء می گردند، به میزان مطلوبی از حافظه، نیاز خواهد بود. برای اجرای چندین برنامه به صورت همزمان و یا اجرای برنامه هایی که میزان بالائی از حافظه را نیاز دارند، ویندوز ۲۰۰۳ امکان حمایت تا ۶۴ و ۱۲۸ گیگابایت را فراهم می نماید.
- **Symmetric Multiprocessing**: سیستم های عامل از ویژگی فوق، به منظور استفاده همزمان از چندین پردازنده استفاده می نمایند. بدین ترتیب کارآیی سیستم بهبود و یک برنامه در محدوده زمانی کمتری اجراء خواهد شد. ویندوز ۲۰۰۳، امکان حمایت (با توجه به نوع نسخه) از حداکثر ۳۲ پردازنده را فراهم می نماید.
- **Plug & Play**: با استفاده از ویندوز ۲۰۰۳، دستگاههایی از نوع PNP به سادگی نصب می گردند. دستگاههای PNP، دستگاههایی هستند که پس از اتصال به سیستم، بدون نیاز به انجام فرآیندهای پیچیده، نصب خواهند شد. پس از اتصال چنین دستگاههایی، ویندوز ۲۰۰۳ به صورت اتوماتیک آنان را تشخیص و عناصر مورد نیاز را نصب و پیکربندی مربوطه را انجام خواهد داد.
- **Clustering**: ویندوز ۲۰۰۳، امکان گروه بندی مستقل کامپیوتر ها را با یکدیگر و به منظور اجرای یک مجموعه از برنامه ها فراهم می نماید. این گروه به عنوان یک سیستم برای سرویس گیرندگان و برنامه ها در نظر گرفته خواهد شد. **چنین گروه بندی، Clustering نامیده شده و گروه هایی از کامپیوتر ها را کلاستر می گویند**. این نوع سازماندهی کامپیوتر ها، باعث برخورد مناسب در صورت بروز اشکال در یک نقطه می گردد. در صورتیکه یک کامپیوتر دچار مشکل گردد، کامپیوتر دیگر در کلاستر، سرویس مربوطه را ارائه خواهد داد.
- **File System**: ویندوز ۲۰۰۳، از ۳ نوع مختلف سیستم فایل (قدیمی و جدید) حمایت میکند: FAT (File Allocation Table)، FAT32 و NTFS (New Technology File System). در صورتی که نیازی به استفاده از

قابلیت های بوت دوگانه (راه اندازی سیستم از طریق دو نوع متفاوت سیستم عامل با توجه به خواسته کاربر) وجود نداشته باشد، ضرورتی به استفاده از سیستم فایل FAT و یا FAT32 وجود نخواهد داشت. NTFS، سیستم فایل پیشنهادی برای ویندوز ۲۰۰۳ بوده و امکانات امنیتی مناسبی را ارائه می نماید. ویندوز ۲۰۰۳، با استفاده از سیستم NTFS امکانات متعددی نظیر: بازیافت سیستم فایل، اندازه پارتیش های بالا، امنیت، فشرده سازی و Disk Quotas (سهمیه بندی دیسک) را ارائه می نماید.

- **Quality of Service (QoS):** امکان QoS، مجموعه ای از سرویس های مورد نظر به منظور حصول اطمینان از انتقال داده ها با یک سطح قابل قبول کیفیت در یک شبکه است. با استفاده از QoS، می توان نحوه پهنای باند اختصاصی به یک برنامه را کنترل نمود. QoS، یک سیستم مناسب، سریع و تضمین شده برای اطلاعات در شبکه را فراهم می نماید.
- **Terminal Service:** با استفاده از ویژگی فوق، امکان دستیابی از راه دور به یک سرویس دهنده از طریق یک ترمینال شبیه سازی شده، فراهم می گردد. یک ترمینال شبیه سازی شده، برنامه ای است که امکان دستیابی به یک کامپیوتر از راه دور را به گونه ای فراهم می نماید که تصور می شود شما در کنار سیستم به صورت فیزیکی قرار گرفته اید (نوعی پیشرفته از Remote Desktop). با استفاده از سرویس ترمینال، می توان برنامه های سرویس گیرنده را بر روی سرویس دهنده اجراء و بدین ترتیب کامپیوتر سرویس گیرنده به عنوان یک ترمینال ایفای وظیفه خواهد کرد (نه به عنوان یک سیستم مستقل). بدین ترتیب هزینه مربوط به عملیات و نگهداری شبکه کاهش و می توان مدیریت سرویس دهنده را از هر مکانی بر روی شبکه انجام داد.
- **Remote Installation Services (RIS):** سرویس فوق، امکان بکارگیری سیستم عامل در یک سازمان توسط مدیران سیستم را تسریع و بهبود خواهد بخشید. بدین ترتیب نیاز به ملاقات فیزیکی هر یک از کامپیوتر های سرویس گیرنده وجود نداشته و می توان از راه دور، اقدام به نصب نمود. سرویس فوق، یک عنصر انتخابی بوده و به عنوان بخشی از نسخه Windows 2003 Server است.

۵-۵- انواع نسخه های ویندوز سرور ۲۰۰۳

1. Web Edition
2. Standard Edition
3. Enterprise Edition
4. Data Center Edition

۵-۵-۱- Server 2003 Web Edition

این نسخه از ویندوز سرور ۲۰۰۳ تا 2 GB حافظه RAM و در صورتی که سخت افزار شما پشتیبانی کند تا ۲ عدد CPU را به صورت **متقارن** (Symmetric) پشتیبانی می کند. این نسخه بیشتر در شبکه برای Web Server یا Application Server استفاده می شود و نمی توان به عنوان Domain Controller یا DHCP و یا FAX Server در نظر گرفته شود.

نکته: در اینجا مفهوم Symmetric و Asymmetric را می گوییم تا در ادامه کار اگر جایی استفاده کردیم دچار ابهام نشویم. در صورتی که در کامپیوتر خود ۲ یا تعداد بیشتری CPU داشته باشیم چه به صورت Dual Core و یا به طور کل دو CPU مجزا از هم، زمانی که دو CPU همزمان با یکدیگر کار می کنند و هر نوع دستورالعمل یا برنامه ای توسط هر یک اجرا می شود و محدودیتی در نوع دستورالعمل ها نمی باشد به این نوع CPU ها متقارن یا Symmetric می گویند و در صورتی که برای هر کدام از CPU ها یک سری دستورالعمل خاص تعریف شده باشد، به طور مثال یک CPU فقط دستورالعمل های سیستمی و CPU دیگر درخواستها و برنامه های کاربر را اجرا کند به این نوع پردازنده ها، نا متقارن یا Asymmetric می گویند.

۵-۵-۲- Server 2003 Standard Edition

این نسخه از ویندوز سرور ۲۰۰۳ تا 4 GB حافظه RAM و تا ۴ عدد CPU را به صورت **متقارن** پشتیبانی می کند. این نسخه معمولاً در شبکه های محلی استفاده می شود و می تواند به عنوان Web Server و یا Application Server و یا Mail Server مورد استفاده قرار گیرد. البته این مسئله را در نظر بگیرید که مطمئنا نسخه Web Edition برای راه انداختن Web Server دارای کارایی و Performance بهتری می باشد چرا که بسیاری از سرویس هایی که در Web Edition استفاده نمی شوند Stop شده اند و این مسئله سرعت سیستم را تا حد قابل توجهی بالا برده است.

۵-۵-۳- Server 2003 Enterprise Edition

نسخه ۳۲ بیتی Enterprise تا 32 GB حافظه RAM و تا ۸ عدد CPU و نسخه ۶۴ بیتی آن تا 64GB حافظه RAM و تا ۸ عدد CPU را پشتیبانی می کنند. قدرت پردازش این Platform در حالت کلی بیشتر از نسخه Standard می باشد.

۵-۵-۴- Server 2003 Datacenter Edition

این نسخه از ویندوز سرور ۲۰۰۳ نیز در دو نسخه ۳۲ و ۶۴ بیتی عرضه می شود. نسخه ۳۲ بیتی در حالت کلی تا 64 GB حافظه RAM و تا ۳۲ عدد CPU را به صورت متقارن پشتیبانی می کند. اما نسخه ۶۴ بیتی این ویندوز تا 512 GB حافظه RAM و تا ۱۲۸ عدد CPU را به صورت **متقارن** پشتیبانی می کند. در جاهایی که بخواهیم حجم بسیار سنگینی را جا به جا کنیم از این نسخه استفاده می کنیم. (که باید بگویم که نسخه ۶۴ بیتی این ویندوز بر روی CPU های Itanuim اجرا می شود).

۵-۶- مقایسه در یک نگاه

ویژگی	Web Server	Server	Enterprise Server	Datacenter Server
کلاستر‌ینگ	خیر	خیر	2 - way	4 - way
حمایت از VPN	محدود	بلی	بلی	بلی
سرویس Internet Authentication	خیر	بلی	بلی	بلی
Network Bridging	خیر	بلی	بلی	بلی
حمایت از Active Directory	فقط Domain Member	Domain Member or Domain Controller	Domain Member or Domain Controller	Domain Member or Domain Controller
حمایت از MetaDirectory Service	خیر	خیر	بلی	خیر
حمایت از SharePoint Team Service	خیر	بلی	بلی	بلی
Removable & Remote Storage	خیر	بلی	بلی	بلی
Fax Services	خیر	بلی	بلی	بلی
Remote Installation Service	خیر	بلی	بلی	بلی
نسخه ۶۴ بیتی برای	خیر	خیر	بلی	بلی

کامپیوتر های Itanium				
Hot -Add Memory Capacity	خیر	خیر	بلی	بلی
Internet Connection Firewall	خیر	خیر	بلی	بلی
حمایت از Public Key Infrastructure (PKI)	محدود	بلی	بلی	بلی
Terminal Service Application Server) (mode	خیر، فقط Remote admin	بلی	بلی	بلی
حداکثر حافظه اصلی	۲ گیگا بایت	۴ گیگا بایت	۳۲ گیگا بایت ------ کامپیوتر های Itanium حداکثر ۶۴ گیگا بایت	۶۴ گیگا بایت ------ کامپیوتر های Itanium حداکثر ۱۲۸ گیگا بایت
تعداد پردازنده	حداقل: ۱ حداکثر: ۲	حداقل: ۱ حداکثر: ۲	حداقل: ۱ حداکثر: ۸	حداقل: ۸ حداکثر: ۳۲

۵-۷- ویژگی های جدید ویندوز سرور ۲۰۰۸

۵-۷-۱- قابلیت ایجاد محیط مجازی

قابلیت Hyper-V ویندوز سرور (نسل جدید تکنولوژی محیط مجازی Hypervisor-Based سرور) به شما امکان می دهد تا چند سرور با وظایف متفاوت در شبکه را توسط راه اندازی ماشین های مجازی مجزا روی یک ماشین فیزیکی واحد ادغام کرده و از این طریق از دارایی های سخت افزاری سرور خود بهترین استفاده را ببرید. همچنین شما می توانید سیستم عامل های مختلف مانند ویندوز، لینوکس و ... را به صورت همزمان روی یک سرور واحد اجرا نمایید. برنامه های کاربردی هم می توانند با استفاده از تکنولوژی های دسترسی متمرکز شده به برنامه های کاربردی در ویندوز سرور ۲۰۰۸ به صورت موثری از مجازی سازی استفاده نمایند. با اجرای Terminal Services Gateway و Terminal Services RemoteApp روی Terminal Server، شما به راحتی اجازه خواهید یافت بدون نیاز به اتصال VPN، از هر کجا به برنامه های استاندارد بر مبنای ویندوز دسترسی داشته باشید.

۵-۷-۲- ساخته شده برای وب

ویندوز سرور ۲۰۰۸ به همراه IIS 7.0 به بازار عرضه می گردد که وب سروری با پلتفرمی ساده و امن برای توسعه و میزبانی مطمئن سرویس ها و برنامه های کاربردی وب می باشد. تغییر مهمی که در پلتفرم وب ویندوز (IIS 7.0) داده شده آن است که **به منظور کنترل و انعطاف بیشتر، از معماری طبقه بندی شده استفاده می کند**. همچنین IIS 7.0 از امکان مدیریت آسان و مکانیزم تشخیص و رفع عیب بسیار قدرتمندی بهره می برد که موجب کاهش اتلاف زمان و افزایش توسعه پذیری همه جانبه می گردد. IIS7.0 به همراه .NET Framework 3.0 پلتفرم جامعی برای ساخت برنامه های کاربردی که ارتباط بین کاربران و داده ها را برقرار می کنند، فراهم می آورد و آنها را قادر می سازد اطلاعات مورد نیاز را ببینند، به اشتراک بگذارند و بر روی آنها عملیات انجام دهند. به علاوه IIS 7.0 در یکپارچه سازی دیگر پلتفرم های وب شرکت مایکروسافت نظیر ASP.NET, Windows Communication Foundation Web Services, Windows SharePoint یک نقش اساسی را ایفا می کند.

۵-۷-۳- امنیت بالا

ویندوز سرور ۲۰۰۸ امن ترین ویندوز ارائه شده تا کنون می باشد. این سیستم عامل به منظور محافظت در **برابر خرابی ها** بسیار مقاوم شده است و از تکنولوژی های جدید متفاوتی برای **ممانعت از برقراری ارتباطات غیر مجاز** به شبکه، سرور ها، داده ها و حسابرسی کاربران شما استفاده کرده است. سرویس Network Access Protection به شما کمک می کند مطمئن شوید کامپیوتر هایی که جهت اتصال به شبکه شما تلاش می کنند با سیاست های امنیتی سازمان متبوع شما مطابقت دارند. ادغام تکنولوژی های مختلف و چندین مورد بهبود در Active Directory، آن را به ابزاری یکپارچه و قدرتمند برای راهکارهای شناسایی هویت و کنترل مبدل کرده است. در پایان سرویس های Read-Only Domain Controller و BitLocker Drive Encryption به شما اجازه می دهند تا Active Directory را به صورت کاملاً امن در محل شعبات خود راه اندازی نمایید.

۵-۷-۴- انجام محاسبات با کارایی بالا

مزایا و امکان کاهش هزینه ها در ویندوز سرور ۲۰۰۸ با توسعه آن توسط Windows HPC Server 2008 که برای محیط های با نیاز محاسباتی بالا طراحی شده است نمود بیشتری می یابد. ویندوز HPC سرور ۲۰۰۸ روی ویندوز های سرور ۲۰۰۸ با تکنولوژی x64-bit ساخته شده است و می تواند بطور موثری با استفاده از عملکرد Out-Of-The-Box به هزاران هسته پردازشی گسترش یافته و در نتیجه کارایی محیط HPC شما را افزایش داده و پیچیدگی آن را کاهش دهد. ویندوز HPC سرور ۲۰۰۸ با تجمیع توانایی کاربران یکپارچه و توانا و تبدیل کامپیوتر های رومیزی به کلاستر های بزرگ، شما را قادر به گسترش همه جانبه می نماید و مجموعه جامعی از ابزارهای گسترش، مدیریت و نظارت را شامل می شود که گسترش، مدیریت و تجمیع با زیرساخت های موجود شما را ساده تر می کند.

۵-۸- لینوکس

سیستم عامل لینوکس بر عکس سیستم عامل ویندوز سرور، به صورت پیش فرض خدمات و نرم افزارهای شبکه ای را با خود به همراه ندارد (البته ویندوز سرور نیز به صورت پیش فرض تمام امکانات شبکه ای را نصب نمی کند ولی در خود دارا می باشد)، و لذا در لینوکس، شما بایستی خودتان نرم افزارها و سرویس های مورد نیاز را نصب نمایید. سیستم عامل های شکل گرفته بر پایه لینوکس، به دلیل پایداری و انعطاف، گزینه های خوبی برای نصب بر روی سیستم های سرور هستند.

۵-۸-۱- نرم افزارهای Server تحت لینوکس

نمونه نرم افزارهای مشهوری که معمولاً تحت لینوکس به عنوان نرم افزار Server استفاده می شوند:

- سرور پروکسی-کش (Proxy-Cache)

- بایند (BIND)
- سرور سامانه نام دامنه (DNS)
- آپاچی (APACHE)
- سرور وب
- پست فیکس(Postfix)
- سرور پست الکترونیکی
- مای اس کیوال (MySQL)
- سرور پایگاه داده
- اسکوئید (SQUID)

۵-۸-۲- ویژگی های اصلی لینوکس چیست؟

۱. چند کاربره بودن (Multi user)
۲. چند وظیفه ای بودن (Multi-Tasking)
۳. واسط کاربر گرافیکی (X windows system)
۴. سرویس دهنده های شبکه (Network Server)
۵. پشتیبانی برنامه های کاربردی (Application Support)
۶. پشتیبانی (Support)
۷. اتصالات شبکه ای (Network Connectivity)

- **چند کاربره بودن**

سیستم عامل لینوکس می تواند به چندین کاربر، اجازه کار کردن با سیستم را بدهد و لذا برای هر کاربر حساب کاربری جداگانه ای را تعریف می کند. ضمنا چندین کاربر می توانند به صورت همزمان به سیستم وارد شوند و در آن مشغول به کار شوند.

- **چند وظیفه ای بودن**

در لینوکس این امکان وجود دارد که چندین برنامه در یک لحظه اجرا شوند؛ یعنی یک کاربر می تواند از چندین برنامه به صورت همزمان استفاده نماید.

- **واسط کاربر گرافیکی**

کاربران مبتدی، ترجیح می دهند از طریق رابط گرافیکی از لینوکس استفاده نمایند. دو رابط گرافیکی GNOME و KDE متداول ترین رابط های گرافیکی برروی این سیستم عامل می باشند.

- **سرویس دهنده های شبکه**

سیستم عامل لینوکس برای کاربردهای شبکه توسعه یافته به طوری که می تواند به عنوان سیستم عامل سرور برای مدیریت منابع مختلف موجود روی شبکه پیکربندی شود.

- **پشتیبانی برنامه های کاربردی**

به خاطر سازگاری لینوکس با استاندارد های صنعتی سیستم عامل، محدوده وسیعی از نرم افزار ها برای لینوکس در دسترس می باشند. معمولاً در سی دی نسخه های مختلف لینوکس، برنامه های کاربردی فراوانی وجود دارند که بسیاری از نیازهای عمومی کاربران را برآورده می سازند.

- **پشتیبانی**

جامعه Open Source و برخی از شرکت های تولید کننده نسخه های لینوکس، از این سیستم عامل پشتیبانی دارند و اگـر در کار با لینوکس دچار مشکل شدید، عملیات پشتیبانی را انجام خواهند داد.

- **اتصالات شبکه**: پشتیبانی از انواع مختلف واسط شبکه (سیمی و بی سیم)

۵-۸-۳- مزایای لینوکس چیست؟

۱. رایگان بودن
۲. قابلیت اعتماد
۳. منابع اطلاعاتی لینوکس در اینترنت

۵-۸-۴- اجزای سیستم عامل لینوکس

سیستم عامل لینوکس دارای سه قسمت اصلی: هسته، محیط و ساختار فایل است.

- **هسته**

هسته بخش اصلی لینوکس است و ارتباط میان سیستم عامل لینوکس و نرم افزارهای نصب شده بر روی آن با سخت افـزار را برقرار می کند. به عبارت دیگر، اجرای برنامه ها و مدیریت سخت افزارها را برعهده دارد.

- **محیط**

محیط نیز واسطی را برای کاربران ایجاد و دستورات کاربران را دریافت نموده و آنها را برای اجرا به هسته ارسال می کنـد. هـر برنامه ای که با هسته ارتباط برقرار می کند، برنامه ای است که در حالت کاربر (User Mode) اجرا می شود.

- **ساختار فایل**

ساختار فایل، نحوه ذخیره شدن فایل ها بر روی دیسک سخت را تعیین می کند. در لینوکس نیز همانند ویندوز، فایـل هـا در داخل دایرکتوری ها قرار می گیرند و کاربران می توانند دایرکتوری ها و فایلهای مورد نظر خود را ایجاد کنند و سپس برای هر یک از آنها مجوز های دسترسی تعیین نمایند.

۵-۸-۵- نسخه های مختلف سیستم عامل لینوکس

1. BlueCat
2. Caldera OpenLinux
3. Debian
4. Ubuntu
5. Dragon Linux
6. Mandrak
7. Red Hat
8. Slackware
9. SUSE
10. Fedora Core

فصل ۶

انواع تجهیزات شبکه

در این فصل، به معرفی تجهیزات سخت افزاری شبکه خواهیم پرداخت.

کابل شبکه – Cable
کارت واسط شبکه – NIC
تکرار کننده – Repeater
هاب – HUB
سوئیچ – Switch
پل – Bridge
دروازه – Gateway
مسیر یاب – Router

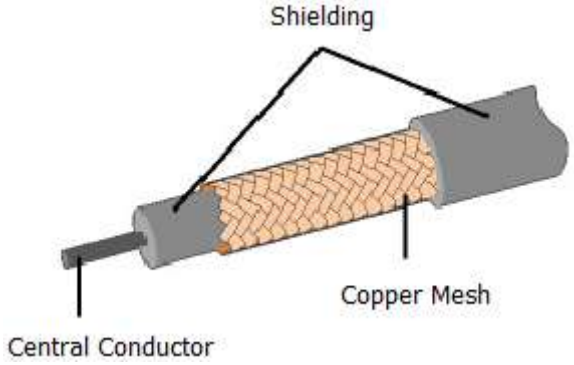
۶-۱- کابل شبکه

۶-۱-۱- انواع رسانه ها

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

۶-۱-۲- کابل کواکسیال

یکی از مهمترین محیط های انتقال در مخابرات کابل کواکسیال و یا هم محور می باشد. این نوع کابل ها از سال ۱۹۳۶ برای انتقال اخبار و اطلاعات در دنیا به کار گرفته شده اند. در این نوع کابل ها، دو سیم تشکیل دهنده یک زوج، از حالت متقارن خارج شده و هر زوج از یک سیم در مغز و یک لایه مسی بافته شده در اطراف آن تشکیل می گردد. ماده ای پلاستیکی این دو هادی را از یکدیگر جدا می کند و مانع از تماس دو هادی در تمام طول کابل با یکدیگر می شود.



مزایای کابل های کواکسیال:

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

معایب کابل های کواکسیال:

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

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

۶-۱-۳- کابل UTP (Unshielded Twisted Pair)

متداولترین نوع کابلی که در انتقال اطلاعات استفاده می گردد، کابل های به هم تابیده می باشند. این نوع کابل ها دارای دو رشته سیم به هم پیچیده بوده که هر دو نسبت به زمین دارای یک امپدانس یکسان می باشند. بدین ترتیب امکان تاثیر پذیری این نوع کابل ها از کابل های مجاور و یا سایر منابع خارجی کاهش خواهد یافت.

کابل های بهم تابیده دارای دو مدل متفاوت: STP (Shielded Twisted Pair) و UTP (Unshielded Twisted Pair) می باشند. کابل UTP نسبت به کابل STP به مراتب متداول تر بوده و در اکثر شبکه های محلی استفاده می گردد.

کیفیت کابل های UTP متغیر بوده و با توجه به مشخصه ها و سطوح کارایی به گروه های خاصی، طبقه بندی میشوند (Category). هرچه درجه بندی طبقه یک کابل بالاتر باشد به این معنی است که آن کابل بهتر است و می تواند داده ها را با سرعت بالاتری ارسال کند.

جدول دسته بندی کابل های UTP

موارد استفاده	سرعت انتقال اطلاعات	گروه
سیستم های قدیمی تلفن، ISDN و مودم	حداکثر تا یک مگابیت در ثانیه	CAT1
شبکه های Token Ring	حداکثر تا چهار مگابیت در ثانیه	CAT2
شبکه های Token Ring و 10BASE-T	حداکثر تا ده مگابیت در ثانیه	CAT3
شبکه های Token Ring	حداکثر تا شانزده مگابیت در ثانیه	CAT4
اترنت (ده مگابیت در ثانیه)، اترنت سریع (یکصد مگابیت در ثانیه) و شبکه های Token Ring (شانزده مگابیت در ثانیه)	حداکثر تا یکصد مگابیت در ثانیه	CAT5
شبکه های Gigabit Ethernet	حداکثر تا یک هزار مگابیت در ثانیه	CAT5e
شبکه های Gigabit Ethernet	حداکثر تا یک هزار مگابیت در ثانیه	CAT6

مزایای کابل های بهم تابیده:

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

معایب کابل های بهم تابیده:

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

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

جدول زیر، اطلاعات کاملی در خصوص کابل های بهم تابیده یا UTP ارائه می دهد:

جدول انواع مدل های کابل UTP

نوع	نرخ انتقال	فرکانس	بیشترین طول	تعداد جفت	کاربرد
Cat1	1 Mbps	1 MHz	90 meters	1 pair	Telephone and ISDN
Cat2	4 Mbps	1 MHz	90 meters	2 pairs	Token ring
Cat3	10 Mbps	16 MHz	100 meters	3 or 4 pairs	10BaseT (Can reach 100 Mbps with 100VGAnyLAN)
Cat4	16 Mbps	16 MHz	100 meters	4 pairs	Token ring
Cat5	10 Mbps 1 Gbps if using all 4 pairs	100 MHz	100 meters	4 pairs	10BaseT and 100BaseT 155 Mbps ATM Gigabit Ethernet
Cat5e	1000 Mbps	100 MHz	100 meters	4 pairs	Gigabit Ethernet
Cat6	4-10 Gbps	250 MHz	100 meters	4 pairs	Gigabit Ethernet, uses all 4 pairs

به یاد داشته باشید که یکی دیگر از تفاوت های موجود بین طبقه های مختلف UTP، تعداد زوج سیم های موجود در کابل می باشد. در ضمن هر جفت سیم رنگ بندی خاصی دارد که مطابق استانداردهای خاصی تعریف شده اند.

به عنوان مثال، کابل Cat5 که امروزه متداولترین نوع کابل UTP می باشد دارای ۴ جفت زوج سیم می باشد که رنگ بندی آنها عبارتند از:

جفت۱: آبی و سفید آبی

جفت۲: نارنجی و سفید نارنجی

جفت ۳: سبز و سفید سبز

جفت۴: قهوه ای و سفید قهوه ای

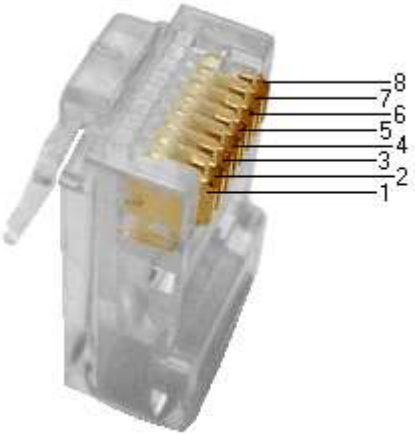
اصول کابل کشی:

کابل کشی شبکه یکی از مراحل مهم در زمان پیاده سازی یک شبکه کامپیوتری است که می بایست با دقت، ظرافت خاص و پایبندی به اصول کابل کشی ساخت یافته، انجام شود. با رعایت اصول کابل کشی ساخت یافته، در صورت بروز اشکال در شبکه، تشخیص و اشکال زدائی آن با سرعتی مناسبی انجام خواهد شد.

اترنت عموما با استفاده از هشت کابل هادی به همراه هشت پین ماژولار Plugs/Jacks، داده را حمل می کند. کانکتور استاندارد، RJ-45 نامیده شده و مشابه کانکتور استاندارد RJ-11 است که در تلفن استفاده می گردد. یک رشته کابل CAT5 شامل چهار زوج سیم بهم تابیده است که هر زوج دارای دو رشته سیم با رنگ هایی خاص است. (یک رشته رنگی و یک رشته سفید و رنگ رشته زوج مربوط). زوج های در نظر گرفته شده برای Ethernet10 و Ethernet100 به رنگ نارنجی و سبز می باشند. از دو زوج دیگر (رنگ قهوه ای و آبی) نیز 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 AT&T، 258A)، استفاده می گردد. تنها تفاوت موجود بین آنان ترتیب اتصالات است.

نحوه شماره گذاری سوکت RJ-45



شماره پین های استاندارد T568B (کلاس B):

همانگونه که در جدول زیر مشاهده می گردد، شماره پین های فرد همواره سفید بوده که با یک نوار رنگی پوشش داده می شوند.

کد رنگ ها در استاندارد T568B		
کاربرد	رنگ	شماره پین
TxData +	سفید/ نارنجی	یک
TxData –	نارنجی	دو
RecvData +	سفید / سبز	سه
	آبی	چهار
	سفید /آبی	پنج
RecvData –	سبز	شش
	سفید/قهوه ای	هفت
	قهوه ای	هشت

شماره پین های استاندارد T568A (کلاس A):

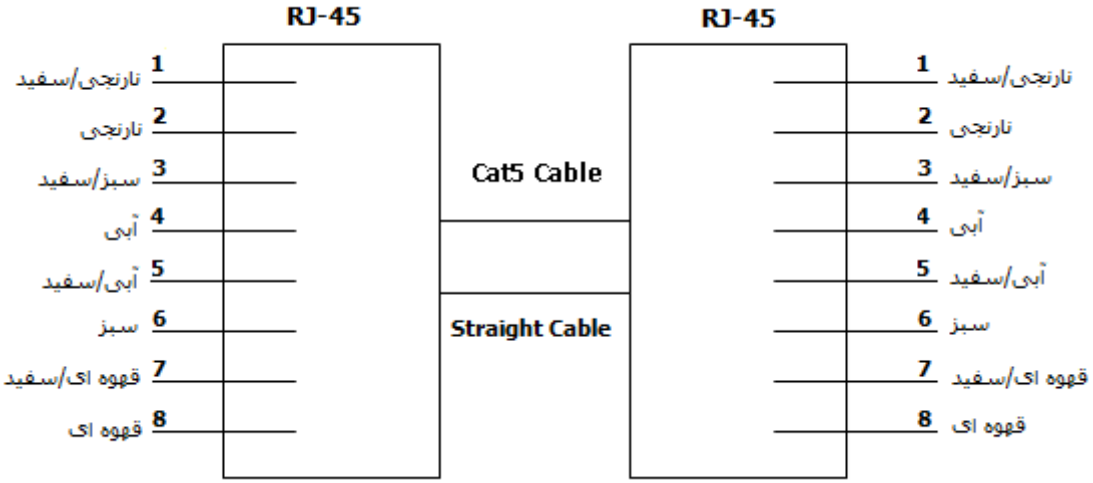
در استاندارد T568A، اتصالات سبز و نارنجی برعکس شده است، بنابراین زوج های یک و دو بر روی چهار پین وسط قرار می گیرند.

کد رنگ ها در استاندارد T568A		
کاربرد	رنگ	شماره پین
+RecvData	سفید/ سبز	یک
–RecvData	سبز	دو
+TxData	سفید / نارنجی	سه
	آبی	چهار
	سفید /آبی	پنج
–TxData	نارنجی	شش
	سفید/قهوه ای	هفت
	قهوه ای	هشت

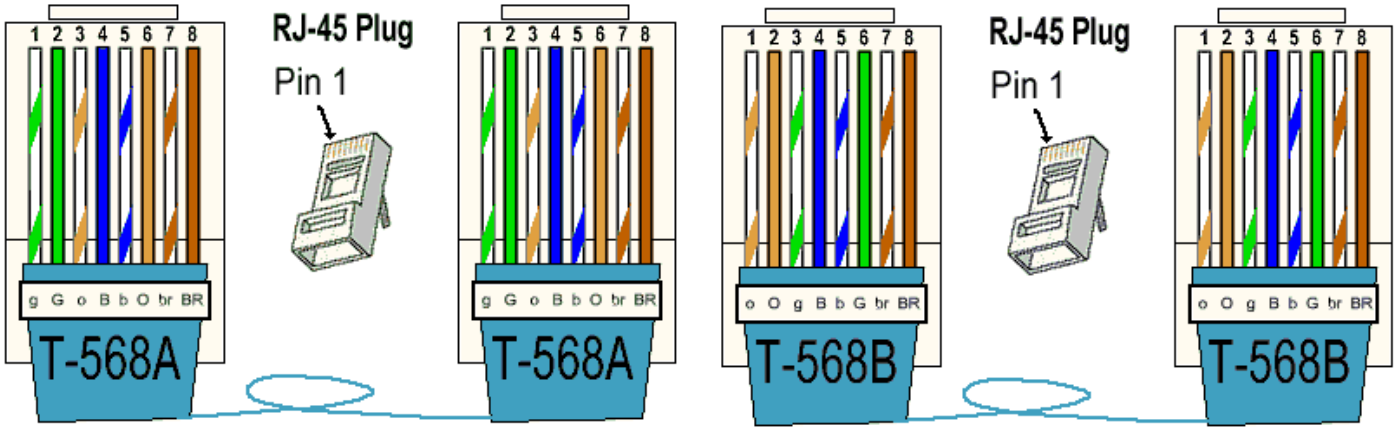
ایجاد یک کابل Straight

متداولترین کاربرد یک کابل Straight، اتصال بین یک **کامپیوتر و هاب/سوئیچ** است.

شکل زیر یک اتصال استاندارد Straight در کابل های CAT5 را نشان می دهد که از آن به منظور اتصال یک PC به هاب و یا سوئیچ استفاده می گردد. البته همانطور که در شکل زیر نیز مشاهده می کنید رنگ بندی و آرایش هر دو سر کابل CAT5 متناظر و مطابق استاندارد T568B صورت گرفته است.



البته کابل های Straight را به صورت T568A نیز می توان ایجاد نمود.



ایجاد کابل Cross-Over

کابل های کراس CAT5 UTP که از آنان با نام Cross-Over نیز نام برده می شود، یکی از متداولترین کابل های استفاده شده پس از کابل هایStraight 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. به عبارت دیگر، هاب عملیات Cross-Over را به صورت داخلی انجام می دهد، در زمانی که یک کامپیوتر را به یک هاب متصل می نماییم، صرفاً 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 Cross-Over را به صورت دستی انجام داد و کابل مختص آن را ایجاد نمود.

چرا به کابل های Cross-Over نیاز داریم؟

در زمان مبادله داده بین دو دستگاه (مثلاً کامپیوتر) ، یکی از آنان به عنوان دریافت کننده و دیگری به عنوان فرستنده ایفای وظیفه می نماید. تمامی عملیات ارسال داده از طریق کابل های شبکه انجام می شود. یک کابل شبکه از چندین رشته سیم دیگر تشکیل می گردد. از برخی رشته سیم ها به منظور ارسال داده و از برخی دیگر به منظور دریافت داده استفاده می شود. برای ایجاد یک کابل Cross-Over از رویکرد فوق استفاده شده و TX (ارسال) یک سمت به RX (دریافت) سمت دیگر، متصل می گردد. شکل زیر نحوه انجام این عملیات را نشان می دهد:

کابل CAT5 Cross-Over

به منظور ایجاد کابل های کراس CAT5 صرفاً از یک روش استفاده می گردد. همانگونه که قبلاً اشاره گردید، یک کابل Cross-Over پین TX یک سمت را به پین RX سمت دیگر متصل می نماید (و برعکس). شکل زیر شماره پین های یک کابل CAT5 معمولی Cross-Over را نشان می دهد.

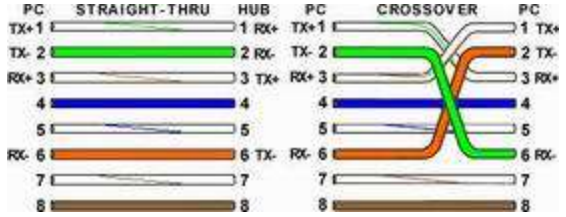
همانگونه که در شکل فوق مشاهده می گردد در کابل های Cross-Over صرفاً از **پین های شماره یک، دو، سه و شش** استفاده می گردد. پین های یک و دو به منزله یک زوج بوده و پین های سه و شش زوج دیگر را تشکیل می دهند. از پین های چهار، پنج، هفت و هشت استفاده نمی گردد. (صرفاً از چهار پین برای ایجاد یک کابل Cross-Over، استفاده می گردد.)

موارد استفاده از کابل های Cross-Over

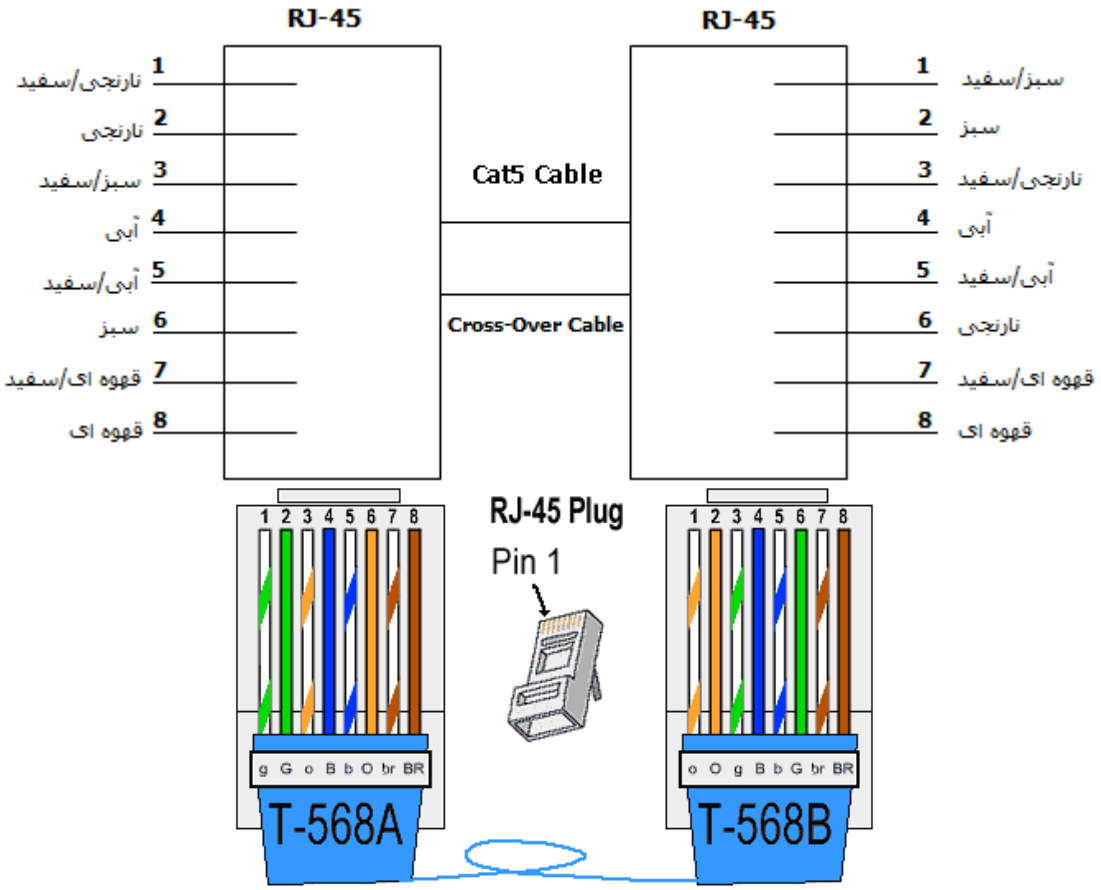
از کابل های Cross-Over **صرفاً** به منظور اتصال دو کامپیوتر استفاده نمی شود و می توان از آنان در دستگاه های متفاوتی نظیر سوئیچ و یا هاب نیز استفاده نمود. در صورتی که قصد داشته باشیم دو هاب را به یکدیگر متصل نماییم، معمولاً از پورت **Uplink** استفاده می گردد. **یعنی پورت های Uplink دو هاب را توسط یک کابل Straight به هم وصل می کنیم**. شکل زیر نحوه اتصال دو هاب به یکدیگر با استفاده از یک کابل Straight و از طریق پورت Uplink را نشان می دهد:

با توجه به وجود پورت Uplink، نیازی به استفاده از یک کابل Cross-Over نخواهد بود. به عبارت دیگر پورت های Uplink از داخل و به طور سخت افزاری، عمل Cross را انجام می دهند. در صورتی که امکان استفاده از پورت Uplink وجود نداشته باشد و بخواهیم دو هاب را با استفاده از پورت های معمولی به یکدیگر متصل نماییم، می توان از یک کابل Cross-Over استفاده نمود. شکل زیر نحوه اتصال دو هاب به یکدیگر با استفاده از یک کابل Cross-Over را و بدون استفاده از پورت Uplink نشان می دهد:

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



به عبارت دیگر، برای ایجاد یک کابل Cross کافیست رنگ بندی یک سر کابل را مطابق استاندارد کلاس A و رنگ بندی سر دیگر کابل را مطابق استاندارد کلاس B، در نظر گرفته و سوکت بزنید. به این ترتیب سیم های ارسال در هر طرف به سیم های دریافت در طرف دیگر منتهی می شوند و برعکس.



۶-۱-۴- آموزش سوکت زنی

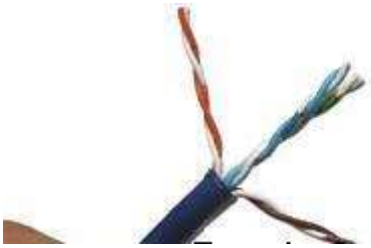
برای سوکت زنی کابل شبکه به تجهیزات زیر نیاز داریم:

۱. کابل شبکه Cat-5

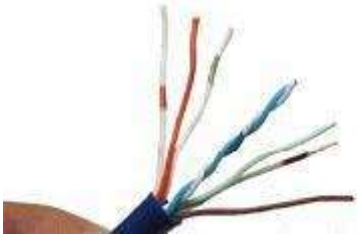
۲. سوکت کابل شبکه

۳. آچار شبکه (دستگاه سوکت زن)

ابتدا مانند شکل زیر، کابل را لخت می کنیم:



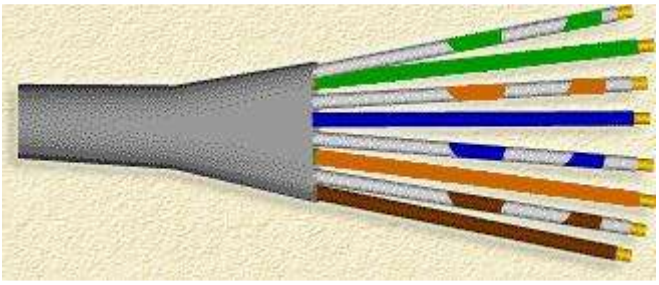
هشت تا سیم داریم که اول دو به دو به هم پیچیده شده است و سپس شده چهار جفت. مجددا این چهار جفت هم دوباره دور هم پیچیده اند. اول جفت ها را از هم جدا کنید:



حالا هر کدام از جفت ها را هم باز کنید و خوب صافشان کنید:

حالا باید سیم ها رو طبق استاندارد کنار هم بچینید.۲ تا استاندارد برای ترتیب رنگی کابل داریم. یکی 568-A کـه عکسـش را در پایین می بینید و به ترتیب از چپ به راست:

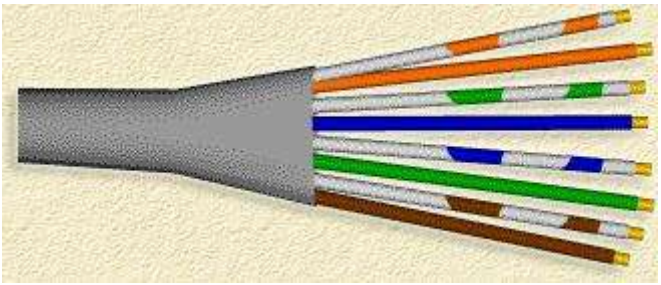
سفید/سبز – سبز - سفید/نارنجی – آبی - سفید/آبی – نارنجی - سفید/قهوه ای - قهوه ای



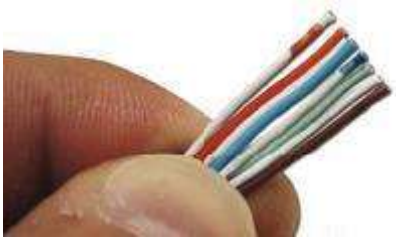
استاندارد بعدی 568-B است که رنگ هایش به این ترتیب از چپ به راست است (تصویر پایین):

سفید/نارنجی – نارنجی - سفید/سبز – آبی - سفید/آبی – سبز - سفید/قهوه ای - قهوه ای

نکته: در حالی که این دو استاندارد با هم فرقی ندارند، ولی استاندارد دوم (568-B) را بیشتر استفاده می کنند.



حالا که استانداردها را یاد گرفتیم، سیم ها را به ترتیب استاندارد کنار هم می چینیم و با انگشت شصت و سبابه پایین سیم ها را نگه میداریم تا بهم نریزد.



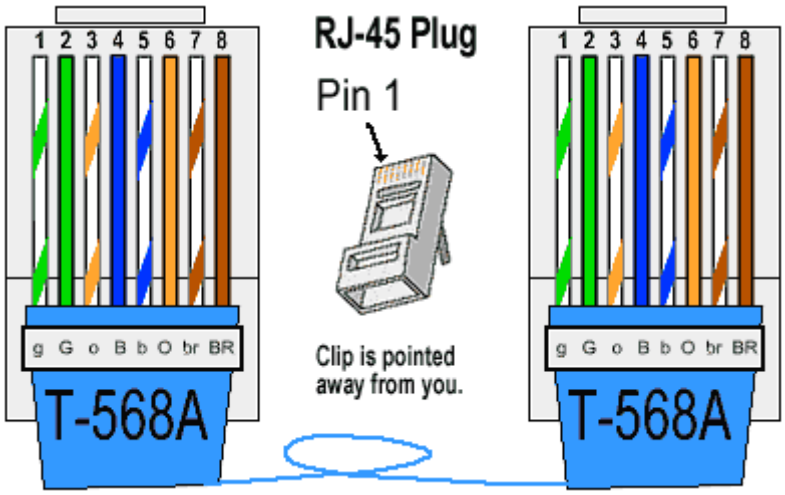
حالا سر سیم ها را به اندازه ۳ سانتی متر و به طور ۹۰ درجه قطع می کنیم تا صاف و یکدست بشود.

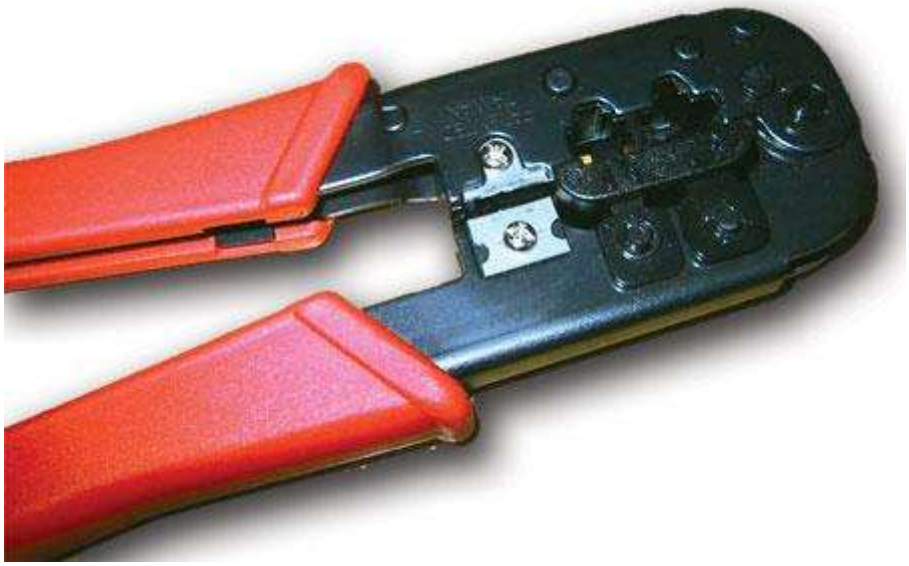
حالا سوکت را طوری در دست می گیریم که ضامنش پایین باشد و با دقت در حالی که زیر سیم را محکم نگه داشته ایم، درون سوکت جا می زنیم به طوری که هر سیم درون شیار خودش قرار بگیرد.

به دقت سوکت را بررسی کرده و مطمئن شوید که سیم ها مرتب و یکسان تا ته سوکت رفته باشند. ضمنا رنگ ها را هم چک کنید که احیانا جابجا نرفته باشد.

انتهای سوکت، فلز های تیغ مانندی هست که بعد از پرس شدن، درون سیم ها فرو رفته و اتصال الکتریکی را برقرار می کند.

در ترتیب رنگ ها بایستی توجه داشته باشید که می خواهید کابل خود را به صورت Cross تولید کنید یا Straight که در بالا توضیح داده ایم. شکل زیر نوعی کابل Cross است.





حالا وقت آن رسیده است که سوکت را با آچار شبکه پرس کنید. بدین منظور سوکت را در محل تعبیه شده داخل آچار قرار داده و سپس آچار را محکم فشار دهید.

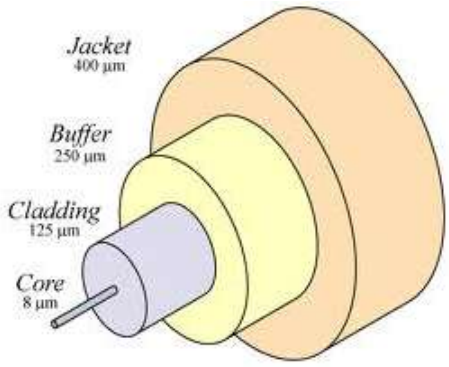
نکته ۱: اگه هر دو سر کابل را با یکی از استانداردهای A یا B ببندید، از این کابل میتوانید برای اتصال کامپیوتر به سوییچ یا مودم/روتر استفاده کنید (نوع Straight).

نکته ۲: اگه یکی از سرها را A و دیگری را B ببندید، اصطلاحا یک کابل کراس آور یا کراس یا همون ضربدری دارید و با آن میتوانید ۲ تا کامپیوتر رو بدون نیاز به سوییچ به هم شبکه کنید (نوع Cross).

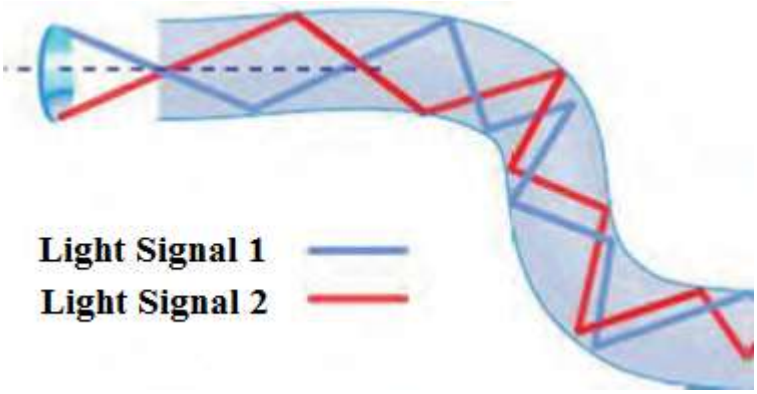
۶-۱-۵- فیبر نوری

یکی از جدیدترین محیط های انتقال در شبکه های کامپیوتری، فیبر نوری است. کابل فیبر نوری برخلاف همه کابل هایی که تاکنون بحث کردیم، بر اساس سیگنال های الکتریکی که در هادی مسی جریان می یابند، نمی باشد؛ بلکه در کابل فیبر نوری از پالس های نور (فوتون ها) برای ارسال سیگنال های باینری تولید شده توسط منبع نورانی (دیود لیزری و یا دیودهای ساطع کننده نور) استفاده می شود. از آنجا که کابل فیبر نوری از نور به جای الکتریسیته استفاده می کند، تقریباً هیچ یک از مشکلات ذاتی کابل مسی همچون تداخل الکترومغناطیسی و نیاز به زمین کردن را ندارد.

کابل فیبر نوری از یک میله استوانه ای که **هسته** نامیده می شود و جنس آن از **سیلیکات** است تشکیل می گردد. شعاع استوانه بین دو تا سه میکرون است. روی هسته، استوانه دیگری (از همان جنس هسته) که **غلاف** نامیده می شود، استقرار می یابد. ضریب شکست هسته را با M1 و ضریب شکست غلاف را با M2 نشان داده و همواره M1>M2 است. در این نوع فیبرها، نور در اثر انعکاسات کلی در فصل مشترک هسته و غلاف، انتشار پیدا خواهد کرد.



در شکل زیر نحوه شکست نور را مشاهده می نمایید:



مزایای فیبر نوری:

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

معایب فیبر نوری:

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

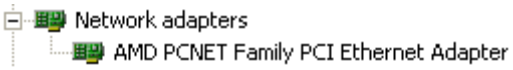
۶-۲- کارت واسط شبکه (NIC)

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

اکثر مادربورد های امروزی که از آنان در کامپیوتر های شخصی استفاده می گردد، دارای یک کارت شبکه OnBoard می باشند. کامپیوتر های قدیمی و یا کامپیوتر های جدیدی که دارای اینترفیس شبکه ای OnBoard نمی باشند، در زمان اتصال به شبکه، می بایست بر روی آنان یک کارت شبکه نصب گردد.

شکل زیر یک نمونه کارت شبکه را که دارای یک پورت RJ-45 است را نشان می دهد.

کامپیوتر ها جهت اتصال به هم و استفاده از برنامه های هم و اشتراک برنامه ها از نظر سخت افزاری احتیاج به کارت شبکه یا LAN Card دارند. که بطور معمول در بازار دو نوع کارت معمول می باشد. یک قسم آنها کارت های ۱۰ در ۱۰ بوده و قسم دیگر کارتهای ۱۰ در ۱۰۰ میباشند. جهت کنترل اتصال درست کارت شبکه به کامپیوتر می توانید روی آیکون My Computer کلیک راست نموده و از قسمت Properties پوشه Device Manager را انتخاب نمایید. در بین ابزارهای نصب شده طبق شکل باید در قسمت Network Adapters، نام و مشخصات کارت شبکه شما وجود داشته باشد.



اگر در این بخش علامت سوال یا تعجب به شکل زرد رنگ وجود داشته باشد، نشان می دهد که راه انداز (Driver) کارت شبکه شما ناقص بوده و درست نصب نشده است و بایستی طبق روش های Hardware Settings آنرا برداشته (Remove) و مجددا نصب نمایید و یا از قسمت Add New Hardware در بخش Control Panel، درایور یا راه انداز مناسب و صحیح آن را نصب نمایید. توجه نمایید که بعد از نصب کارت شبکه، آیکون Network Neighborhood در روی میز کار (Desktop) مشاهده خواهد شد. از آنجایی که ما معمولاً دو نوع شبکه **BNC و HUB** را مورد استفاده قرار می دهیم بر روی اکثر کارت ها جهت اتصال هر دو نوع رابط وجود دارد. کارت های OnBoard، معمولا فقط جای HUB را دارند.

۶-۲-۱- وظایف کارت شبکه

۱. برقراری ارتباط لازم بین کامپیوتر و محیط انتقال

۲. **تبدیل داده:** داده ها بر روی گذرگاه (Bus) کامپیوتر به صورت موازی حرکت می نمایند. نحوه حرکت داده ها بر روی محیط انتقال شبکه به صورت سریال است. ترانسیور کارت شبکه (یک ارسال کننده و یا دریافت کننده)، داده ها را از حالت موازی به سریال و بالعکس تبدیل می نماید.

۳. **ارائه یک آدرس منحصر به فرد سخت افزاری:** آدرس سخت افزاری (MAC) درون تراشه ROM موجود بر روی کارت شبکه نوشته می گردد. آدرس MAC در واقع یک زیر لایه از لایه Data Link مدل مرجع OSI می باشد. آدرس سخت افزاری موجود بر روی کارت شبکه، یک آدرس منحصر به فرد را برای هر یک از کامپیوتر های موجود در شبکه،

مشخص می نماید. پروتکل هایی نظیر TCP/IP از یک سیستم آدرس دهی منطقی (آدرس IP)، استفاده می نمایند. در چنین مواردی قبل از دریافت داده توسط کامپیوتر، می بایست آدرس منطقی به آدرس سخت افزاری ترجمه گردد.

۴. **کپسوله کردن داده ها:** کارت شبکه و درایور آن مجموعاً قبل از انتقال اطلاعات باید داده هایی را که توسط پروتکل لایه شبکه تولید شده است، در یک فریم کپسوله کنند. عمل دیگری که کارت شبکه در این زمینه انجام می دهد خواندن محتوای فریم های دریافت شده از شبکه و انتقال داده های آنها به پروتکل مناسب در لایه شبکه می باشد.

۵. **کد گذاری و کد گشایی سیگنال ها:** کارت شبکه مسئول پیاده سازی روش کد گذاری لایه شبکه می باشد که در آن اطلاعات باینری تولید شده در لایه شبکه که حالا در فریم، کپسوله شده است را به بارهای الکتریکی یعنی ولتاژ های الکتریکی، پالس های نور یا هر نوع سیگنالی که رسانه شبکه استفاده می کند تبدیل می کند. از طرف دیگر کارت شبکه سیگنال های دریافتی از شبکه را برای پروتکل های لایه بالاتر به اطلاعات باینری تبدیل می کند.

۶. **دریافت و انتقال اطلاعات:** مهمترین وظیفه کارت شبکه تولید و ارسال سیگنال های مناسب روی شبکه و دریافت سیگنال های موجود در شبکه می باشد. ماهیت سیگنال ها به رسانه شبکه و پروتکل لایه پیوند-داده بستگی دارد. در LAN های متداول امروزی، هریک از کامپیوتر های موجود در شبکه همه بسته های فرستاده شده روی شبکه را دریافت می کنند و سپس کارت شبکه آدرس مقصد لایه پیوند-داده هر یک از آنها را بررسی می کند تا بسته هایی که به مقصد آن کامپیوتر تولید شده اند را برای پردازش به لایه بعدی از پشته پروتکل منتقل کند، در غیر اینصورت بسته دور انداخته می شود.

۷. **بافر کردن داده ها:** کارت های شبکه هر زمان فقط یک فریم داده را روی شبکه می فرستند یا از آن دریافت می کنند، بنابراین در خود بافری دارند که تا زمان کامل و آماده شدن یک فریم برای پردازش، داده هایی که از طرف کامپیوتر یا شبکه در یافت می کنند را ذخیره کنند.

۸. **تبدیل سریال به موازی و برعکس:** ارتباطات بین کامپیوتر و کارت شبکه به صورت موازی انجام می شود، مگر در کارتهای شبکه USB که ارتباط با کامپیوتر در آنها به صورت سریال است. اما ارتباطات شبکه ای به صورت سریال انجام می شوند، بنابراین کارت شبکه مسئول تبدیل این دو نوع روش انتقال اطلاعات به همدیگر می باشد.

روند نصب یک کارت شبکه، شامل قراردادن کارت داخل کامپیوتر، پیکربندی کارت برای استفاده از منابع سخت افزاری مناسب، و نهایتا نصب درایور کارت می باشد که بسته به توانایی ها و نوع کامپیوتر از نظر قدیمی یا جدید بودن این پروسه می تواند بسیار ساده و یا بسیار پر دردسر باشد.

توجه: قبل از لمس کردن قطعات داخلی کامپیوتر یا درآوردن کارت شبکه از بسته محافظ مخصوص آن، دست خود را با ورقه فلزی دور منبع تغذیه کامپیوتر تماس دهید یا اینکه از دستکش های مخصوص استفاده کنید تا به دلیل تخلیه الکترواستاتیکی به قطعات آسیبی وارد نشود.

۶-۲-۲- انواع کارت شبکه

واسط شبکه کابل های UTP به شکل سوکت RJ-45 و برای کابل های کواکسیال، کانکتور BNC یا AUI می باشد، البته در بعضی موارد می توان از فرستنده های بی سیم هم استفاده کرد.

کارت شبکه به کمک درایور خود موظف به انجام اغلب **وظایف پروتکل های لایه پیوند-داده و فیزیکی** می باشد و زمان خرید باید کارت متناسب با پروتکلی که برای لایه پیوند-داده انتخاب کرده اید (مثل اترنت یا Token Ring) را خریداری کنید و توجه داشته باشید که این دو نوع کارت را نمی توان به جای یکدیگر استفاده کرد. نکته دیگری که زمان خرید باید مورد توجه قرار گیرد انتخاب کارتی است که علاوه بر تناسب با پروتکل لایه پیوند-داده، از گونه مورد نظر آن پروتکل هم پشتیبانی کند.

فراموش نکنید که کارت شبکه منتخب شما باید با اسلات باس کامپیوتری که قرار است در آن نصب شود، متناسب باشد و دارای کانکتور مخصوص رسانه شبکه باشد.

غیر از کارت های شبکه ای که مختص اتصال کامپیوتر ها به شبکه های محلی سرویس گیرنده /دهنده استاندارد هستند، انواع دیگری وجود دارند که کامپیوتر ها و دستگاه های دیگر را به شبکه های بخصوصی بنام شبکه ذخیره ناحیه ای یا **SAN** (Storage Area Network) متصل می کنند. یک SAN شبکه ای مجزا است که مختص ارتباطات بین سرور ها و دستگاههای ذخیره سازی خارجی، از قبیل RAID می باشد. اغلب کارت های شبکه SAN بجای اترنت و Token Ring از پروتکل دیگری بنام Fiber Channel استفاده میکنند.

برای اتصال کارت شبکه به Motherboard نیز دو نوع اسلات PCI و ISA داریم. اسلات های PCI به مراتب از اسلات های ISA سریع تر هستند و دارای قابلیت خود پیکربندی می باشند، بنابراین کارت هایی که از این استاندارد استفاده می کنند متداول ترند.

اما در صورتیکه کامپیوتر تان فقط دارای اسلات ISA باشد به ناچار می توانید از کارت های شبکه ISA استفاده کنید. در سیستم های قابل حمل تنها انتخاب، کارت های PC Card می باشد. این نوع کارت ها مختص اسلات های PCMCIA می باشند و در این نوع اسلات ها قرار می گیرند. اما در صورتیکه سیستم شما از استاندارد CardBus پشتیبانی می کند، زمان خرید باید کارتی را انتخاب کنید که آن هم از این استاندارد پشتیبانی کند. CardBus استانداردی است که برای لوازم جانبی PC Card، بازدهی معادل بازدهی استاندارد PCI مهیا میکند.

در بازار کارت های شبکه ای که از پورت USB برای اتصال به کامپیوتر استفاده می کنند هم وجود دارد، اما رابط USB قدیمی، حداکثر می تواند در سرعت ۱.۲ مگابیت در ثانیه کار کند که حتی در مقایسه با استاندارد ISA کند است. همیشه سرعت انتقال داده در کارت شبکه شما باید با تجهیزات دیگر شبکه متناسب باشد.

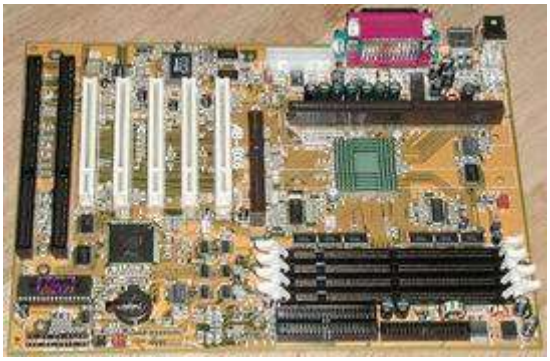
کارت های شبکه متناسب با نوع کابلی که پشتیبانی می کنند دارای انواع مختلف کانکتور می باشند. بعضی از NIC ها (کارت های شبکه) بیش از یک کانکتور کابل دارند که شما را قادر به انتخاب رسانه شبکه مطلوب می کنند. به عنوان مثال، کارت هایی وجود دارند که دارای سه کانکتور AUI، BNC و RJ45 می باشند و **کارت مرکب** نامیده می شوند. این نوع کارت ها از کارت هایی که فقط یک کانکتور دارند به مراتب گران ترند. توجه داشته باشید که همزمان فقط از یکی کانکتور ها می توانید استفاده نمایید.

۶-۲-۳- انتخاب کارت شبکه

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

- **سازگاری با معماری استفاده شده در شبکه**: کارت های شبکه دارای مدل های متفاوتی با توجه به معماری استفاده شده در شبکه (اترنت، Token ring) می باشند. اترنت، متداولترین معماری شبکه در حال حاضر است که در شبکه هایی با ابعاد بزرگ و کوچک، استفاده می گردد.
- **سازگاری با Throughput شبکه**: در صورتی که یک شبکه اترنت سریع (سرعت 100 Mbps) پیاده سازی شده است، انتخاب یک کارت اترنت با سرعت 10 Mbps تصمیم مناسبی در این رابطه نخواهد بود. اکثر کارت های شبکه جدید قادر به سوئیچینگ اتوماتیک بین سرعت های 10 و 100 Mbps می باشند (اترنت معمولی و اترنت سریع)
- **سازگاری با نوع اسلات های خالی مادربورد**: کارت های شبکه دارای مدل های متفاوتی با توجه به نوع اسلات مادربورد می باشند. کارت های شبکه PCI درون یک اسلات خالی PCI و کارت هایی از نوع ISA در اسلات های ISA نصب می گردند. کارت شبکه می بایست متناسب با یکی از اسلات های خالی موجود بر روی مادربورد، انتخاب گردد. اسلات آزاد به نوع مادربورد بستگی داشته و در این رابطه گزینه های متعددی نظیر ISA,PCI و EISA می تواند وجود داشته باشد.

شکل زیر یک نمونه مادربورد را که دارای اسلات های ISA و PCI است، نشان می دهد:



۶-۲-۴- ساختار کارت واسط شبکه (NIC)

کارت های شبکه از نظر ساختاری به چند دسته تقسیم بندی میشوند. از لحاظ استاندارد مورد استفاده سه نوع کارت شبکه وجود دارند این دسته بندی بر اساس نحوه ارتباط با مادربورد به شرح زیر است:

1. ISA/EISA: Architecture Standard Industry / Extended ISA
2. PCI Peripheral Components Industry :
3. USB: Universal Synchronous Bus

- **ISA:** تجهیزات ISA تا سالهای ۱۹۹۹ و ۲۰۰۰ تولید می شدند. اما این تجهیزات به دلیل نواقصی زیادی که داشت با شکست مواجه شد. دو دلیل عمده این شکست به شرح زیر است:

۱. اسلات های ISA ی نصب شده روی مادربورد با نصف سرعت Bus مادربورد کار می کردند؛ که نتیجه آن کاهش خواندن و فرستادن اطلاعات به RAM بود.

۲. در هر لحظه تنها یک اسلات اجازه استفاده از باس مادربورد را داشت و در صورتیکه دو اسلات همزمان به انتقال داده روی مادربورد می پرداختند، هر دو از عمل خارج میشدند.

- **PCI:** از مزایای این فناوری از بین رفتن دو مشکل عمده تکنولوژی ISA بود. در این فناوری هر اسلات با سرعت باس مادربورد و همزمان با اسلات های دیگر نیز میتوانست کار کند.

- **USB:** کارتهای واسط را میتوان به نوعی سه دسته دانست که دسته سوم استفاده از ورودی های USB می باشد. تکنولوژی استفاده شده در این تجهیزات عینا شبیه به PCI میباشد. (گذرگاه فراگیر(گسترده) همزمان)

دسته بندی شبکه از نظر نوع مبادله اطلاعات:

شبکه سنکرون:

در این روش، هر دو طرف، قابلیت تبادل اطلاعات را دارند.

دو نوع شبکه سنکرون (Synchronous) داریم:

۱- دوطرفه غیر همزمان :

دوطرفه غیر همزمان: کارت شبکه A اطلاعات برای کارت B میفرستد و B تنها زمانی که کارت A فرستادن را تمام کرده است، جواب می دهد مثل برخی LAN ها. (شبکه تلفن بین المللی بیسیم)

۲- دوطرفه همزمان:

همزمان می توانند اطلاعات را بفرستند و بگیرند (تلفن شهری)

شبکه آسنکرون:

در این شبکه داده های ارسالی تنها می توانند از یک مسیر از مبدا به مقصد منتقل شوند و گذرگاه همیشه یکطرفه باقی میماند. اگر A فرستنده و B دریافت کننده باشد، همیشه از A به B انتقال داده صورت میپذیرد. یعنی فقط یک طرفه هستند (مانند رادیو - تلویزیون)

۶-۳- تکرار کننده (Repeater)

وسیله ای در تجهیزات شبکه است که در مدارات ارتباطی (معمولاً شبکه Bus) مورد استفاده قرار می گیرد و تضعیف سیگنال ها را از طریق تقویت یا تولید مجدد آنها کاهش می دهد تا سیگنال ها با همان شکل اول به راه خود ادامه دهند. بدین ترتیب می توان سیگنال را بدون کاستی به فواصل دورتری فرستاد. این وسیله حداکثر فاصله ای را که یک کابل شبکه محلی می تواند گسترده شود افزایش دهد. استفاده از یک تکرارگر یک شبکه محلی را به دو قسمت تقسیم نمی کند و شبکه تقابلی نمی سازد. از آنجا که تکرارگر ها با سیگنال های فیزیکی واقعی سروکار دارند و در جهت تفسیر داده ای که انتقال می دهند تلاشی نمی کنند، این تجهیز در **لایه فیزیکی** یعنی اولین لایه از مدل مرجع OSI عمل می کند.

این وسیله در واقع نوع خاصی از HUB است که فقط دارای ۲ پورت است.

۱. کار تکرارگر تقویت سیگنال های بین دو شبکه یا سگمنت های یک شبکه که فاصله ی زیادی از هم دارند می باشد.

۲. این قطعه در دو نوع Passive و Active قابل دسترس بوده است:

۱.۲. Passive Repeater: این نوع Repeater دو تا پورت دارد که هر یک به یک کابل شبکه متصل هستند و سیگنالی که از یک کابل دریافت کرده است از خود عبور می دهد و بر روی کابل دیگر می فرستد. به این ترتیب هیچگونه تغییری در سیگنال به وجود نیامده و تقویتی صورت نگرفته است بلکه Repeater مانند یک کانکتور (اتصال دهنده) عمل می کند و نیاز به منبع تغذیه و برق ندارد.

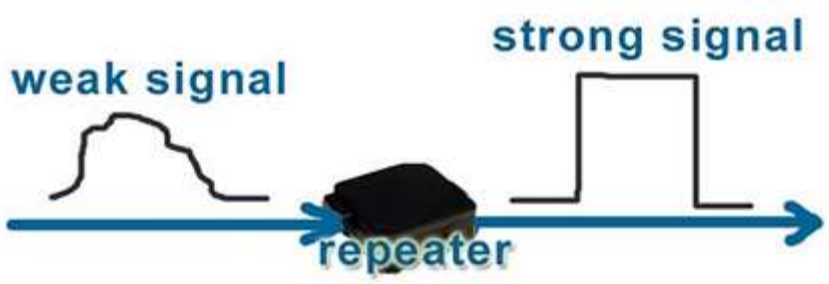
۲.۲. Active Repeater: در این نوع Repeater سیگنال دریافت شده را مجددا تقویت و بازسازی می کند، به طوری که به نظر می رسد که سیگنال جدید است. البته برای انجام چنین عملیاتی نیاز به منبع تغذیه و برق دارد.

به یاد داشته باشید که عملکرد Repeater ها صرفاً الکتریکی است و در لایه فیزیکی شبکه (لایه اول) عمل می کنند. به عبارت دیگر Repeater ها فقط سیگنال های الکتریکی ورودی را تقویت می کنند و بیرون می دهند و هیچ درکی از داده ها ندارند و قادر به هیچ نوع فیلتر کردن داده ها نیز نیستند.

اما تفاوت های دیگری نیز بین دو مدل Passive و Active وجود دارد:

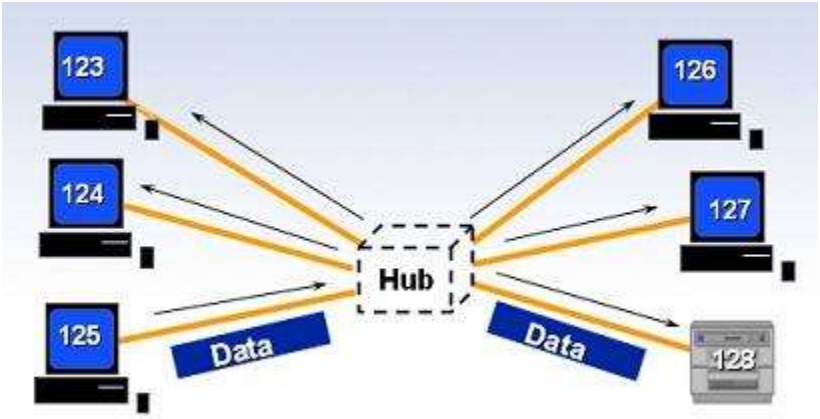
۱. نوع اول علاوه بر سیگنال هر چیز دیگری حتی نویز امواج نا خواسته که به همراه سیگنال اصلی که دارای اطلاعات است می باشند (Passive). مثلاً در امواج صوتی نویزی که باعث افت کیفیت صدا و شنیدن اصوات اضافه می شود را هم تقویت می کند.

۲. اما تکرار کننده ی نوع Active، سیگنال را قبل از ارسال بازدید کرده و چیز های اضافه را خارج می کند و مثلاً دیگر نویز ر ا تقویت نمی کند.

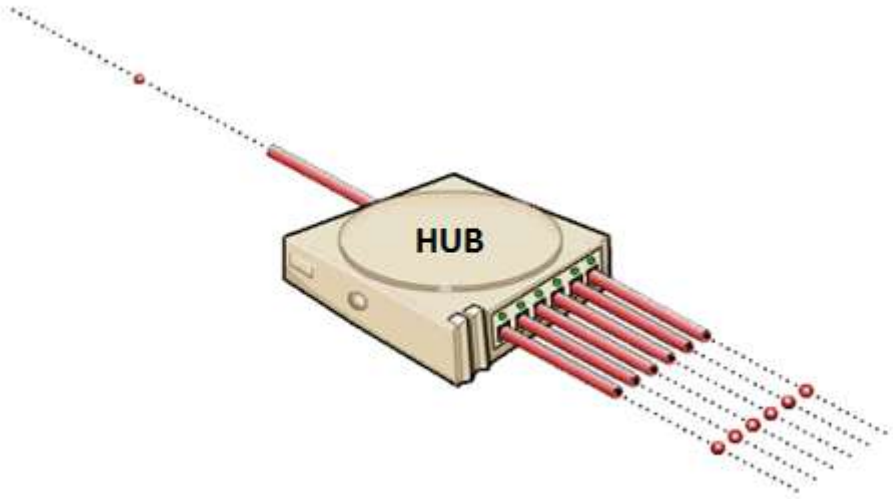


۶-۴- هاب (HUB)

هاب به وسیله ای گفته می شود که خطوط ارتباطی را در یک نقطه مرکزی به یکدیگر متصل می کند و اتصالات مشترکی برای تمامی وسایل فراهم می آورد.



هاب در مرکز شبکه های Star قرار می گیرد و تمام کامپیوتر های موجود در شبکه توسط یک کابل مستقل به آن متصل می شوند. هاب در حقیقت از ترکیب چندین Repeater ساخته شده است به این ترتیب که هریک از پورت های هاب، حکم یک Repeater را دارند. به عبارت دیگر یک پالس ورودی به یکی از پورت های، به همه پورت های خروجی ارسال می شود.



به عبارت دیگر هاب ها، جهت اتصال گروهی از کاربران به یک شبکه محلی به کار می روند. هاب ها، کلیه بسته داده های دریافتی برروی یک درگاه از ایستگاه کاری را (همچون E-mail، اسناد Word، صفحه های گسترده گرافیک ها و درخواست های چاپ) به کلیه پورت های دیگر انتقال می دهند. کلیه کاربران متصل به یک هاب منفرد و یا گروهی از هاب های متصل، در یک "قطعه" قرار دارند، یعنی پهنای باند هاب یا ظرفیت انتقال داده ها را به اشتراک می گذارند. با افزایش تعداد کاربران به "قطعه"، مسئله رقابت برای به دست گرفتن مقدار محدودی از پهنای باند اختصاص یافته به آن قطعه افزایش می یابد.

۶-۴-۱- انواع هاب

سه نوع هاب رایج وجود دارد:

الف - هاب فعال (Active):

که مانند آمپلی فایر عمل می کند و باعث تقویت مسیر عبور سیگنال ها می شود و از تصادم و برخورد سیگنال ها در مسیر جلوگیری به عمل می آورد. این هاب نسبتا قیمت بالایی دارد.

ب - غیر فعال (Passive):

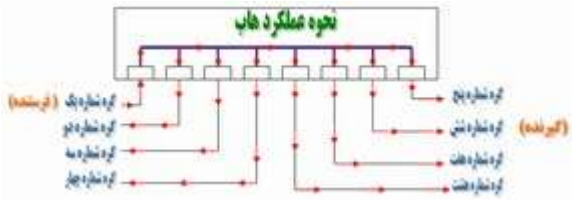
که بر خلاف نوع اول که در مورد تقویت انتقال سیگنال ها فعال است، این هاب منفعل بوده و هیچ برنامه و رفتاری جهت جلوگیری از تصادم ندارد.

ج – آمیخته (Mixed):

که قادر به ترکیب انواع رسانه ها " کابل کواکسیال نازک، ضخیم و.... " و باعث تعامل درون خطی میان سایر هاب ها می شود.

۶-۴-۲- آشنائی با نحوه عملکرد هاب

نحوه کار هاب بسیار ساده است. زمانی که یکی از کامپیوتر های متصل شده به هاب اقدام به ارسال داده ای می نماید، سایر پورت های هاب نیز آن را دریافت خواهند کرد (داده ارسالی تکرار و برای سایر پورت های هاب نیز فرستاده می شود). شکل زیر نحوه عملکرد هاب را نشان می دهد.



همانگونه که در شکل فوق مشاهده می نمائید، گره ۱ داده ای را برای گره ۶ ارسال می نماید، ولی تمامی گره های دیگر نیز داده را دریافت خواهند کرد. در ادامه، بررسی لازم در خصوص داده ارسالی توسط هر یک از گره ها انجام و در صورتی که تشخیص داده شود که داده ارسالی متعلق به آنان نیست، آن را نادیده خواهند گرفت. عملیات فوق از طریق کارت شبکه موجود بر روی کامپیوتر که آدرس MAC مقصد فریم ارسالی را بررسی می نماید، انجام می شود. کارت شبکه بررسی لازم را انجام و در صورت عدم مطابقت آدرس MAC موجود در فریم، با آدرس MAC کارت شبکه، فریم ارسالی دور انداخته می گردد.

اکثر هاب ها دارای یک پورت خاص می باشند که می تواند به صورت یک پورت معمولی و یا یک پورت Uplink رفتار نماید. با استفاده از یک پورت Uplink می توان یک هاب دیگر را به هاب موجود و به کمک کابل Straight، متصل نمود. بدین ترتیب تعداد پورت ها افزایش یافته و امکان اتصال تعداد بیشتری کامپیوتر به شبکه فراهم می گردد. روش فوق گزینه ای ارزان قیمت به منظور افزایش تعداد گره ها در یک شبکه است ولی با انجام این کار شبکه شلوغ تر شده و همواره بر روی آن حجم بالائی داده غیر ضروری در حال جابجائی است.

در اکثر هاب ها از یک LED به منظور نشان دادن فعال بودن ارتباط برقرار شده بین هاب و گره و از LED دیگر به منظور نشان دادن بروز یک Collision (تصادم - تصادف)، استفاده می گردد. (دو LED مجزا). در برخی از هاب ها دو LED مربوط به فعال بودن لینک ارتباطی بین هاب و گره و فعالیت پورت با یکدیگر ترکیب و زمانی که پورت در حال فعالیت است، LED مربوطه چشمک زن شده و زمانی که فعالیتی انجام نمی شود، LED فوق به صورت پیوسته روشن خواهد بود.

LED مربوط به Collision موجود بر روی هاب ها زمانی روشن می گردد که یک Collision به وجود آید. Collision زمانی به وجود می آید که دو کامپیوتر و یا گره سعی نمایند در یک لحظه بر روی شبکه صحبت نمایند. پس از بروز یک Collision، فریم های مربوط به هر یک از گره ها با یکدیگر برخورد نموده و خراب می گردند. هاب به منظور تشخیص این نوع تصادم ها به اندازه کافی هوشمند بوده و برای مدت زمان کوتاهی چراغ مربوط به Collision روشن می گردد. (یک دهم ثانیه به ازای هر تصادم).

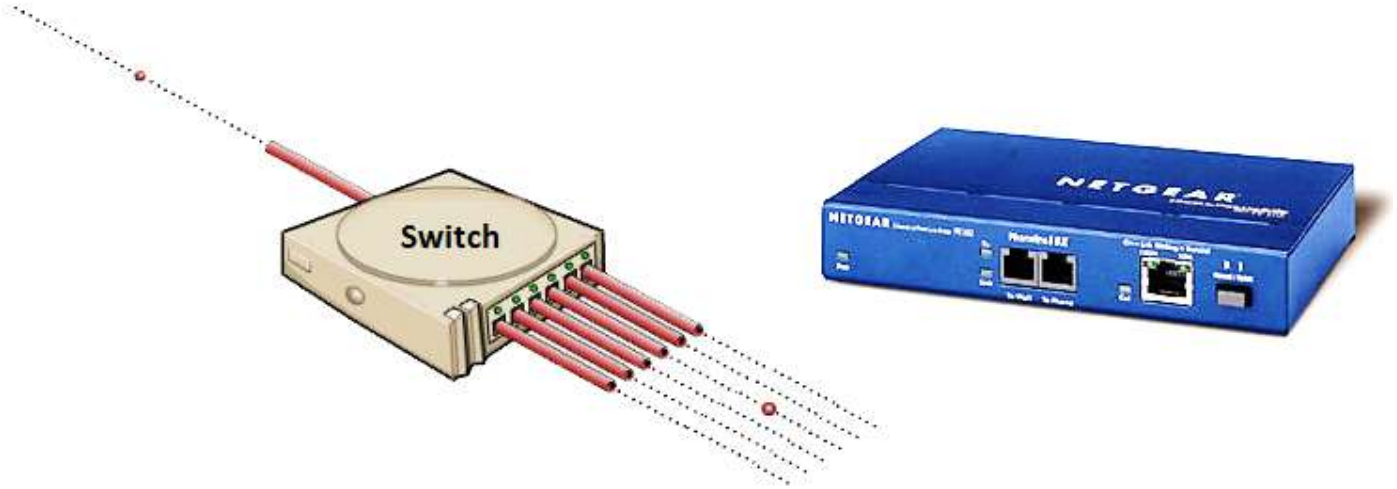
تعداد اندکی از هاب ها دارای یک اتصال خاص از نوع BNC بوده که می توان از آن به منظور اتصال یک کابل کواکسیال، استفاده نمود. پس از اتصال فوق، LED مربوط به اتصال BNC روی هاب روشن می گردد. لازم به ذکر است که این وسیله (HUB) امروزه دیگر تولید نمی شود و به جای آن در شبکه های امروزی از Switch استفاده می گردد.

به یاد داشته باشید که هاب نیز در لایه فیزیکی شبکه کار می کند و ضمن توزیع کردن سیگنال ورودی بین سایر پورت ها، سیگنال ورودی را تقویت نیز می کند. به این ترتیب در شبکه های Star در فواصل دور، برای اتصال کامپیوتر ها به یکدیگر نیز می توان از آن استفاده کرد.

۶-۵- سوئیچ (Switch)

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 (معمولاً کامپیوتر) یک شبکه را مستقیماً با یکدیگر فراهم می نماید. شبکه ها و سوئیچ ها دارای انواع متفاوتی می باشند.



سوئیچ ها، هوشمند تر از هاب ها می باشند و به هر کاربر یا هر گروه از کاربران پهنای باند مشخصی را اختصاص می دهند. سوئیچ، بر اساس اطلاعات موجود در Header هر بسته، بسته داده ها را تنها به پورت گیرنده مورد نظر و متصل به شبکه LAN ارسال می کند. سوئیچ در هر انتقال ویژه باعث ایجاد تماس های فردی و موقت بین منابع و مقاصد شده و پس از اتمام مکالمه، به این تماس خاتمه می دهد.

به عبارت دیگر، سوئیچ وسیله ای است که بسته ها را مستقیماً به پورت های مرتبط با نشانی های خاص شبکه هدایت می کند. سوئیچ ها فهم بیشتری به مدیریت انتقال داده اضافه میکنند.

سوئیچ ها معمولاً در لایه ۲ مدل OSI هستند (سوئیچ لایه ۳ را بعدا توضیح می دهیم) و با تعداد پورت ۵، ۸، ۱۶، ۲۴ و گاهی ۳۶ و ۴۸ پورت نیز تولید می شوند. سرعت آنها معمولاً ۱۰۰/۱۰ و یا ۱۰۰۰ مگابیت بر ثانیه است. سوئیچ ها دارای پورت های RJ-45 و یا فیبر نوری و یا ترکیبی از هر دو هستند. در دو نوع رومیزی و رکمونت (نصب در رک های ۱۹ اینچ استاندارد) وجود دارند.

سوئیچ هایی 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 صرفاً بین دو دستگاه که قصد ارتباط با یکدیگر را دارند، در زمان مورد نظر ایجاد می نماید.

قبل از ادامه مباحث، به معرفی برخی اصطلاحات استفاده شده می پردازیم:

۱- **گره**. گره، شامل هر چیزی که به شبکه متصل می گردد، خواهد بود. (کامپیوتر، چاپگر و...)

۲- **سگمنت**. سگمنت یک بخش خاص از شبکه بوده که توسط یک سوئیچ، روتر و یا Bridge از سایر بخش ها جدا شده است.

۳- **ستون فقرات**. کابل اصلی که تمام سگمنت ها به آن متصل می گردند. معمولاً ستون فقرات یک شبکه دارای سرعت بمراتب بیشتری نسبت به هر یک از سگمنت های شبکه است. مثلاً ممکن است نرخ انتقال اطلاعات ستون فقرات شبکه ۱۰۰ مگابیت در ثانیه بوده در صورتیکه نرخ انتقال اطلاعات هر سگمنت ۱۰ مگابیت در ثانیه باشد.

۴- **توپولوژی**. روشی که هر یک از گره ها به یکدیگر متصل می گردند را گویند.

۵- **آدرس MAC**. آدرس فیزیکی هر دستگاه (کارت شبکه) در شبکه است. آدرس فوق یک عدد شش بایتی بوده که سه بایت اول آن مشخص کننده سازنده کارت شبکه و سه بایت دوم، شماره سریال کارت شبکه است.

۶- **Unicast**. ارسال اطلاعات توسط یک گره با آدرس خاص و دریافت اطلاعات توسط گره دیگر است.

۷- **Multicast**. یک گره، اطلاعاتی را برای یک گروه خاص (با آدرس مشخص یا الگویی خاص) ارسال می دارد. فقط دستگاههای موجود در گروه، اطلاعات ارسالی را دریافت خواهند کرد.

۸- **Broadcast**. یک گره اطلاعاتی را برای تمام گره های موجود در شبکه ارسال می نماید.

۶-۵-۱- استفاده از سوئیچ

در اکثر شبکه های متداول، به منظور اتصال گره ها از هاب استفاده می شود. همزمان با رشد شبکه (تعداد کاربران، تنوع نیازها، کاربردهای جدید شبکه و...) مشکلاتی در شبکه های **هاب** به وجود می آید:

۱. **Scalability**: در یک شبکه مبتنی بر هاب، پهنای باند به صورت مشترک توسط کاربران استفاده می گردد. با توجه به محدود بودن پهنای باند، همزمان با توسعه، کارآیی شبکه به شدت تحت تاثیر قرار خواهد گرفت. برنامه های کامپیوتر که امروزه به منظور اجراء بر روی محیط شبکه، طراحی می گردند به پهنای باند مناسبی نیاز خواهند داشت. عدم تامین پهنای باند مورد نیاز برنامه ها، تاثیر منفی در عملکرد آن ها را بدنبال خواهد داشت.

۲. **Latency**: به مدت زمانی که طول خواهد کشید تا بسته اطلاعاتی به مقصد مورد نظر خود برسد، اطلاق می گردد. با توجه به اینکه هر گره در شبکه های مبتنی بر هاب می بایست مدت زمانی را در انتظار سپری کرده (ممانعت از تصادم اطلاعات)، به

موازات افزایش تعداد گره ها در شبکه، مدت زمان فوق افزایش خواهد یافت. در این نوع شبکه ها در صورتیکه یکی از کاربران فایل با ظرفیت بالائی را برای کاربر دیگر ارسال نماید، تمام کاربران دیگر می بایست در انتظار آزاد شدن محیط انتقال به منظور ارسال اطلاعات باشند. به هرحال افزایش مدت زمانی که یک بسته اطلاعاتی به مقصد خود برسد، هرگز مورد نظر کاربران یک شبکه نخواهد بود.

۳. Network Failure: در شبکه های مبتنی بر هاب، یکی از دستگاههای متصل شده به هاب قادر به ایجاد مسائل و مشکلاتی برای سایر دستگاه های موجود در شبکه خواهد بود. عامل بروز اشکال می تواند عدم تنظیم مناسب سرعت (مثلاً تنظیم سرعت یک هاب با قابلیت ۱۰ مگابیت در ثانیه به ۱۰۰ مگابیت در ثانیه) و یا ارسال بیش از حد بسته های اطلاعاتی از نوع Broadcast، باشد.

۴. Collisions: در شبکه های مبتنی بر تکنولوژی اترنت (Ethernet) از فرآیند خاصی با نام CSMA/CD به منظور ارتباط در شبکه استفاده می گردد. فرآیند فوق نحوه استفاده از محیط انتقال به منظور ارسال اطلاعات را قانونمند می نماید. در چنین شبکه هایی تا زمانی که بر روی محیط انتقال ترافیک اطلاعاتی باشد، گره ای دیگر قادر به ارسال اطلاعات نخواهد بود. در صورتیکه دو گره در یک لحظه اقدام به ارسال اطلاعات نمایند، یک تصادم اطلاعاتی ایجاد و عملاً بسته های اطلاعاتی ارسالی توسط هر یک از گره ها نیز از بین خواهند رفت. هر یک از گره های مربوطه (تصادم کننده) می بایست بمدت زمان کاملاً تصادفی در انتظار باقی مانده و پس از فراهم شدن شرایط ارسال، اقدام به ارسال اطلاعات مورد نظر خود نمایند.

هاب مسیر ارسال اطلاعات از یک گره به گره دیگر را به حداقل مقدار خود می رساند ولی عملاً شبکه را به سگمنت های گسسته تقسیم نمی نماید. سوئیچ به منظور تحقق خواسته فوق عرضه شده است. یکی از مهمترین تفاوت های موجود بین هاب و سوئیچ، تفسیر هر یک از پهنای باند است. تمام دستگاه های متصل شده به هاب، پهنای باند موجود را بین خود به اشتراک می گذارند. در صورتیکه یک دستگاه متصل شده به سوئیچ، دارای تمام پهنای باند مختص خود است. مثلاً در صورتیکه ۱۰ گره به هاب متصل شده باشند، (در یک شبکه ۱۰ مگابیت در ثانیه) هر گره موجود در شبکه بخشی از تمام پهنای باند موجود (۱۰ مگابیت در ثانیه) را اشغال خواهد کرد (یعنی هر یک ۱ مگابیت در ثانیه، البته در صورتیکه سایر گره ها نیز قصد ارتباط را داشته باشند). در سوئیچ، هر یک از گره ها قادر به برقراری ارتباط با سایر گره ها با سرعت ۱۰ مگابیت در ثانیه خواهد بود.

در یک شبکه مبتنی بر سوئیچ، برای هر گره، یک سگمنت اختصاصی ایجاد خواهد شد. سگمنت های فوق به یک سوئیچ متصل خواهند شد. در حقیقت سوئیچ امکان حمایت از چندین (در برخی حالات صدها) سگمنت اختصاصی را دارا است. با توجه به اینکه تنها دستگاه های موجود در هر سگمنت سوئیچ و گره می باشند، سوئیچ قادر به انتخاب اطلاعات، قبل از رسیدن به سایر گره ها خواهد بود. در ادامه، سوئیچ فریم های اطلاعاتی را به سگمنت مورد نظر هدایت خواهد کرد. با توجه به اینکه هر سگمنت دارای صرفاً یک گره می باشد، اطلاعات مورد نظر به مقصد مورد نظر ارسال خواهند شد. بدین ترتیب در شبکه های مبتنی بر سوئیچ امکان چندین مبادله اطلاعاتی به صورت همزمان وجود خواهد داشت.

با استفاده از سوئیچ، شبکه های اترنت به صورت Full-Duplex خواهند بود. قبل از مطرح شدن سوئیچ، اترنت به صورت Half-Duplex بود. در چنین حالتی داده ها در هر لحظه امکان ارسال در یک جهت را دارا می باشند. در یک شبکه مبتنی بر سوئیچ، هر گره صرفاً با سوئیچ ارتباط برقرار می نماید (گره ها مستقیماً 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 کانکتور های 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، صرفاً از سوئیچ به تنهایی استفاده نمی نمایند. در این نوع شبکه ها از ترکیب هاب و سوئیچ استفاده می گردد. مثلاً یک سازمان می تواند از چندین هاب به منظور اتصال کامپیوتر های موجود در هر یک از دپارتمانهای خود استفاده و در ادامه با استفاده از یک سوئیچ تمام هاب ها (مربوط به هر یک از دپارتمان ها) به یکدیگر متصل می گردد.

۶-۵-۲- تکنولوژی سوئیچ ها

سوئیچ ها دارای پتانسیل های لازم به منظور تغییر روش ارتباط هر یک از گره ها با یکدیگر می باشند. تفاوت سوئیچ با روتر چیست؟ سوئیچ ها معمولاً در لایه دوم (Data layer) مدل OSI فعالیت می نمایند. در لایه فوق امکان استفاده از آدرس های MAC (آدرس ها ی فیزیکی) وجود دارد. روتر در لایه سوم (Network) مدل OSI فعالیت می نمایند. در لایه فوق از آدرس های IP ر IPX و یا Apple Talk استفاده می شود. (آدرس های منطقی). الگوریتم استفاده شده توسط سوئیچ به منظور اتخاذ تصمیم در رابطه با مقصد یک بسته اطلاعاتی با الگوریتم استفاده شده توسط روتر، متفاوت است.

یکی از موارد اختلاف الگوریتم های سوئیچ و هاب، نحوه برخورد آنان با Broadcast است. مفهوم بسته های اطلاعاتی از نوع Broadcast در تمام شبکه ها مشابه می باشد. در چنین مواردی، دستگاهی نیاز به ارسال اطلاعات داشته ولی نمی داند که اطلاعات را برای چه کسی می بایست ارسال نماید. به دلیل عدم آگاهی و دانش نسبت به هویت دریافت کننده اطلاعات، دستگاه مورد نظر اقدام به ارسال اطلاعات به صورت Broadcast می نماید. مثلاً هر زمان که کامپیوتر جدید و یا یک دستگاه به شبکه وارد می شود، یک بسته اطلاعاتی از نوع Broadcast برای معرفی و حضور خود در شبکه ارسال می دارد. سایر گره ها قادر به افزودن کامپیوتر مورد نظر در لیست خود و برقراری ارتباط با آن خواهند بود. بنابراین بسته های اطلاعاتی از نوع Broadcast در مواردی که یک دستگاه نیاز به معرفی خود به سایر بخش های شبکه را داشته و یا نسبت به هویت دریافت کننده اطلاعات شناخت لازم وجود نداشته باشند، استفاده می گردند.

هاب و یا سوئیچ ها قادر به ارسال بسته ای اطلاعاتی از نوع Broadcast برای سایر سگمنت های موجود در حوزه Broadcast می باشند. روتر عملیات فوق را انجام نمی دهد. در صورتیکه آدرس یک دستگاه مشخص نگردد، روتر قادر به مسیر یابی بسته اطلاعاتی مورد نظر نخواهد بود. ویژگی فوق در مواردی که قصد جداسازی شبکه ها از یکدیگر مد نظر باشد، بسیار ایده آل خواهد بود. ولی زمانیکه هدف مبادله اطلاعاتی بین بخش های متفاوت یک شبکه باشد، مطلوب به نظر نمی آید. سوئیچ ها با هدف برخورد با مشکل فوق عرضه شده اند.

سوئیچ های LAN بر اساس تکنولوژی Packet-Switching فعالیت می نمایند. سوئیچ یک ارتباط بین دو سگمنت ایجاد می نماید. بسته های اطلاعاتی اولیه در یک محل موقت (بافر) ذخیره می گردند، آدرس فیزیکی (MAC) موجود در هدر خوانده شده و در ادامه با لیستی از آدرس های موجود در جدول Lookup (جستجو) مقایسه می گردد. در شبکه های LAN مبتنی بر اترنت، هر فریم اترنت شامل یک بسته اطلاعاتی خاص است. بسته اطلاعاتی فوق شامل یک عنوان (هدر) خاص و شامل اطلاعات مربوط به آدرس فرستنده و گیرنده بسته اطلاعاتی است.

سوئیچ های مبتنی بر بسته های اطلاعاتی، به منظور مسیر یابی ترافیک موجود در شبکه از سه روش زیر استفاده می نمایند.

1. **Cut-Through**
2. **Store-and-forward**
3. **Fragment-free**

Cut-Through

سوئیچ های Cut-through، بلافاصله پس از تشخیص بسته اطلاعاتی توسط سوئیچ، آدرس MAC خوانده می شود. پس از ذخیره سازی شش بایت اطلاعات که شامل آدرس می باشند، بلافاصله عملیات ارسال بسته های اطلاعاتی به گره مقصد آغاز می گردد. (همزمان با دریافت سایر بسته های اطلاعاتی توسط سوئیچ). با توجه به عدم وجود کنترل های لازم در صورت بروز خطا در روش فوق، سوئیچ های زیادی از روش فوق استفاده نمی نمایند.

Store-and-forward

سوئیچ های Store-And-Forward، تمام بسته اطلاعاتی را در بافر مربوطه ذخیره و عملیات مربوط به بررسی خطا (CRC) و سایر مسائل مربوطه را قبل از ارسال اطلاعات انجام خواهند داد. در صورتی که بسته اطلاعاتی دارای خطا باشد، بسته اطلاعاتی دور انداخته خواهد شد.. در غیر اینصورت، سوئیچ با استفاده از آدرس MAC، بسته اطلاعاتی را برای گره مقصد ارسال می نماید. اغلب سوئیچ ها از ترکیب دو روش گفته شده استفاده می نمایند. در این نوع سوئیچ ها از روش Cut-Through استفاده شده و به محض بروز خطا از روش Store-And-Forward استفاده می نمایند.

Fragment-free

یکی دیگر از روش های مسیر یابی ترافیک در سوئیچ ها که کمتر استفاده می گردد، Fragment-Free است. روش فوق مشابه Cut-Through بوده با این تفاوت که قبل از ارسال بسته اطلاعاتی ۶۴ بایت آن ذخیره می گردد.

۶-۵-۳- انواع سوئیچ LAN

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

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

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

۳- Bus Architecture: در این نوع از سوئیچ ها به جای استفاده از یک شبکه (تور)، از یک مسیر انتقال داخلی (Bus) استفاده و مسیر فوق با استفاده از TDMA توسط تمام پورت ها به اشتراک گذاشته می شود. سوئیچ های فوق برای هر یک از پورت ها دارای یک حافظه اختصاصی می باشند.

۴- Transparent Bridging: اکثر سوئیچ های LAN مبتنی بر اترنت از سیستمی با نام Transparent Bridging برای ایجاد جداول آدرس Lookup استفاده می نمایند. تکنولوژی فوق امکان یادگیری هر چیزی در رابطه با محل گره های موجود در شبکه، بدون حمایت مدیریت شبکه را فراهم می نماید. تکنولوژی فوق داری پنج بخش متفاوت است:

1. **Learning**
2. **Flooding**
3. **Filtering**
4. **Forwarding**
5. **Aging**

نحوه عملکرد تکنولوژی فوق بشرح زیر است:

- سوئیچ به شبکه اضافه شده و تمام سگمنت ها به پورت های سوئیچ متصل خواهند شد.

- گره A بر روی اولین سگمنت (سگمنت A)، اطلاعاتی را برای کامپیوتر دیگر (گره B) در سگمنت دیگر (سگمنت C) ارسال می دارد.

- سوئیچ اولین بسته اطلاعاتی را از گره A دریافت می نماید. آدرس MAC آن خوانده شده و آن را در جدول Lookup سگمنت A ذخیره می نماید. بدین ترتیب سوئیچ از نحوه یافتن گره A آگاهی پیدا کرده و اگر در آینده گره ای قصد ارسال اطلاعات برای گره A را داشته باشد، سوئیچ در رابطه با آدرس آن مشکلی نخواهد داشت. فرآیند فوق را Learning می گویند.

- با توجه به اینکه سوئیچ دانشی نسبت به محل گره B ندارد، یک بسته اطلاعاتی را برای تمام سگمنت های موجود در شبکه (بجز سگمنت A که اخیراً یکی از گره های موجود در آن اقدام به ارسال اطلاعات نموده است.) فرآیند ارسال یک بسته اطلاعاتی توسط سوئیچ، به منظور یافتن یک گره خاص برای تمام سگمنت ها، Flooding نامیده می شود.

- گره B بسته اطلاعاتی را دریافت و یک بسته اطلاعاتی را به عنوان Acknowledgement برای گره A ارسال خواهد کرد.

- بسته اطلاعاتی ارسالی توسط گره B به سوئیچ می رسد. در این زمان، سوئیچ قادر به ذخیره کردن آدرس MAC گره B در جدول Lookup سگمنت C می باشد. با توجه به اینکه سوئیچ از آدرس گره A آگاهی دارد، بسته اطلاعاتی را مستقیماً برای آن ارسال خواهد کرد. گره A در سگمنتی متفاوت نسبت به گره B قرار دارد، بنابراین سوئیچ می بایست به منظور ارسال بسته اطلاعاتی دو سگمنت را به یکدیگر متصل نمائید. فرآیند فوق Forwarding نامیده می شود.

- در ادامه بسته اطلاعاتی بعدی از گره A به منظور ارسال برای گره B به سوئیچ می رسد، با توجه به اینکه سوئیچ از آدرس گره B آگاهی دارد، بسته اطلاعاتی فوق مستقیماً برای گره B ارسال خواهد شد.

- گره C اطلاعاتی را از طریق سوئیچ برای گره A ارسال می دارد. سوئیچ آدرس MAC گره C را در جدول Lookup سگمنت A ذخیره می نماید، سوئیچ آدرس گره A را دانسته و مشخص می گردد که دو گره A و C در یک سگمنت قرار دارند. بنابراین نیازی به ارتباط سگمنت A با سگمنت دیگر به منظور ارسال اطلاعات گره C نخواهد بود. بدین ترتیب سوئیچ از حرکت بسته های اطلاعاتی بین گره های موجود در یک سگمنت ممانعت می نماید. فرآیند فوق را Filtering می گویند.

- Learning و Flooding ادامه یافته و به موازات آن سوئیچ، آدرس های MAC مربوط به گره ها را در جداول Lookup ذخیره می نماید. اکثر سوئیچ ها دارای حافظه کافی به منظور ذخیره سازی جداول Lookup می باشند. به منظور بهینه سازی حافظه فوق، اطلاعات قدیمی تر از جداول فوق حذف تا فرآیند جستجو و یافتن آدرس ها در یک زمان معقول و سریعتر انجام پذیرد. بدین منظور سوئیچ ها از روشی با نام Aging استفاده می نمایند. زمانیکه یک Entry برای یک گره در جدول Lookup اضافه می گردد، به آن یک زمان خاص نسبت داده می شود. هر زمان که بسته ای اطلاعاتی از طریق یک گره دریافت می گردد، زمان مورد نظر بهنگام می گردد. سوئیچ دارای یک زمان سنج قابل پیکربندی بوده که باعث می شود، Entry های موجود در جدول Lookup که مدت زمان خاصی از آنها استفاده نشده و یا به آنها مراجعه ای نشده است، حذف گردند. با حذف Entry های غیر ضروری، حافظه قابل استفاده برای سایر Entry ها بیشتر می گردد.

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

۶-۵-۴- روتر ها و سوئیچینگ لایه سوم

همانگونه که قبلاً اشاره گردید، اکثر سوئیچ ها در لایه دوم مدل OSI فعالیت می نمایند (Data Layer). اخیراً برخی از تولیدکنندگان سوئیچ، مدلی را عرضه نموده اند که قادر به فعالیت در لایه سوم مدل OSI است (Network Layer). این نوع سوئیچ ها دارای شباهت زیادی با روتر می باشند.

زمانی که روتر یک بسته اطلاعاتی را دریافت می نماید، در لایه سوم به دنبال آدرس های مبداء و مقصد گشته تا مسیر مربوط به بسته اطلاعاتی را مشخص نماید. سوئیچ های استاندارد از آدرس های MAC به منظور مشخص کردن آدرس مبداء و مقصد استفاده می نمایند (از طریق لایه دوم). مهمترین تفاوت بین یک روتر و یک سوئیچ لایه سوم، استفاده سوئیچ های لایه سوم از سخت افزارهای بهینه به منظور ارسال داده با سرعت مطلوب نظیر سوئیچ های لایه دوم است. نحوه تصمیم گیری آنها در رابطه با مسیر یابی بسته های اطلاعاتی مشابه روتر است. در یک محیط شبکه ای LAN، سوئیچ های لایه سوم معمولاً دارای سرعتی بیشتر از روتر می باشند. علت این امر استفاده از سخت افزارهای سوئیچینگ در این نوع سوئیچ ها است. اغلب سوئیچ های لایه سوم شرکت سیسکو، به منزله روتر هایی می باشند که به مراتب از روتر ها سریعتر بوده (با توجه به استفاده از سخت

افزارهای اختصاصی سوئیچینگ) و دارای قیمت ارزان تری نسبت به روتر می باشند. نحوه Pattern Matching و Caching در سوئیچ های لایه سوم مشابه یک روتر است. در هر دو دستگاه از یک پروتکل روتینگ و جدول روتینگ، به منظور مشخص نمودن بهترین مسیر استفاده می گردد. سوئیچ های لایه سوم قادر به برنامه ریزی مجدد سخت افزار به صورت پویا و با استفاده از اطلاعات روتینگ لایه سوم می باشند و همین امر باعث سرعت بالای پردازش بسته های اطلاعاتی می گردد. سوئیچ های لایه سوم، از اطلاعات دریافت شده توسط پروتکل روتینگ به منظور بهنگام سازی جداول مربوط به Caching استفاده می نمایند.

همانگونه که ملاحظه گردید، در طراحی سوئیچ های LAN از تکنولوژی های متفاوتی استفاده می گردد. نوع سوئیچ استفاده شده، تاثیر مستقیم بر سرعت و کیفیت یک شبکه را بدنبال خواهد داشت.

۶-۵-۵- سوئیچ های مدیریتی

برای کنترل و نگهداری شبکه های بزرگ و یا شبکه هایی که نیاز به پهنای باند زیاد و کنترل شده دارند نیاز به استفاده از سوئیچ های مدیریتی است. با اینگونه سوئیچ ها می توان تنظیمات متنوعی از قبیل پهنای باند، شبکه های مجازی، کنترل و گزارشات ترافیکی شبکه و... را انجام داد. از مشخصاتی که تقریباً در تمام آنها مشترک است می توان به رکمونت بودن، تعداد ۲۴ پورت به بالا، امکان افزودن چندین نوع ماژول برای کاربردهای مختلف، وجود پورت سریال برای مدیریت مستقیم، امکان مدیریت از طریق وب، دارا بودن نرم افزار مدیریتی، پاور های اضافی و قیمت بسیار بالا نسبت به سوئیچ های رایج اشاره کرد. سرعت سوئیچ کردن داخلی و همچنین حجم داده انتقالی در زمان واحد از جمله مشخصات مهم سوئیچ ها و تعیین کننده قیمت آنها می باشد. برخی از این سوئیچ ها امکان مدیریت در لایه ۲ شبکه و بالاتر را نیز دارند.

۶-۵-۶- ماژول سوئیچ

ماژول ها قطعاتی سخت افزاری هستند که به سخت افزار اصلی متصل شده و امکاناتی را بسته به نیاز شبکه به آن اضافه می نمایند. به سوئیچ هایی که دارای ورودی برای نصب ماژول هستند سوئیچ های ماژولار گفته می شود. جدیدترین ماژول ها، ماژول های SFP یا Mini GIBIC هستند که انواع پورت های گیگابیت بر روی فیبر نوری و کابل مسی ارائه می کنند. سوئیچ ماژولار این امکان را به طراح شبکه میدهد تا بتواند چندین نوع مدیا را در کنار هم داشته باشند.

۶-۵-۷- مزایای سوئیچ

۱. یک سوئیچ اترنت مزایای زیادی دارد، از قبیل اجازه به تعدادی کاربر برای برقراری ارتباط موازی از طریق استفاده از مدار های مجازی و قسمتهای اختصاصی شبکه در یک محیط عاری از برخورد، یعنی از طریق پهنای باند بیشتر آزاد و هر کاربر پهنای باند مخصوص به خود دارد.

۲. مزیت دیگر آن این است که جایگزینی آن با هاب به سادگی انجام پذیر است و نیازی به تعویض سخت افزار و کابل های موجود نمی باشد و بالاخره مدیر شبکه به سادگی میتواند آنرا مدیریت کند.

۳. سوئیچ ها در لایه پیوند داده ای (از لایه های شبکه) کار می کنند و همانند پل ها اجازه اتصال Segment های LAN به یکدیگر برای تشکیل یک شبکه بزرگتر را می دهند.

۴. سوئیچ ها ترافیک را کاهش میدهد و در نتیجه نسبت به دیگر تجهیزات فعال شبکه از سرعت بالاتری برخوردار هستند و می توانند از کاربر های جدیدی همانند LAN (VLAN مجازی) پشتیبانی کنند.

۶-۵-۸- از چه نوع سوئیچ هایی استفاده کنیم؟

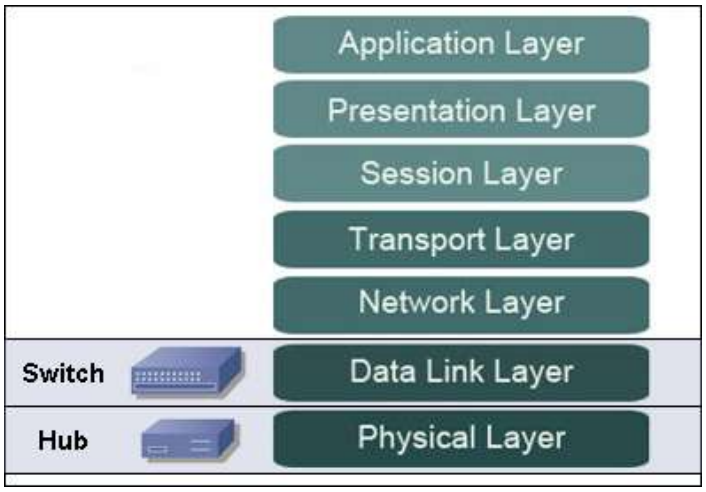
با توجه به طرح توسعه شبکه دولت، مطرح شده از طرف نهاد ریاست جمهوری در راستای اجرای پروژه دولت الکترونیکی که بر اساس فن آوری جدید GIGABIT ETHERNET) 1000 Mbps) طراحی شده، بهتر است در شبکه هایی که هنوز راه اندازی نشده اند و مراحل طراحی را طی می نمایند از سوئیچ هایی با امکانات وجود یک یا دو یا چند پورت فعال 1000 Mbps استفاده نماییم. همچنین در این طرح (شبکه دولت) مسئله امنیت شبکه حائز اهمیت میباشد، به همین دلیل بهتر است یکباره از سوئیچ هایی استفاده نماییم که در آنها یک تکنولوژی جدید بنام IP SECURITY جهت بالا بردن امنیت شبکه بکار گرفته شده است، بدین صورت که امکان تخصیص یک پورت خاص به یک ترمینال خاص را دارد، چنانکه یک تغییر فیزیکی در محل پورت سوئیچ و جابجایی کامپیوتر ها بدون هماهنگی با مدیر شبکه رخ دهد، امکان استفاده از شبکه از بین خواهد رفت.
محل نصب سوئیچ در شبکه در Backbone (کانال اصلی انتقال داده ها) و یا در Gateways (ورودی ها) که دو شبکه را به هم مرتبط می سازند می باشد.

۶-۵-۹- تفاوت HUB با Switch

هاب و سوئیچ در اصل عملکرد یکسانی را انجام می دهند، اگرچه روش های انجام کار آنها متفاوت می باشد. از هر دو آن ها در جهت احیای سیگنال های ضعیف شده استفاده می شود، همچنین هر دو آن ها توانایی تقسیم و جداسازی یک سیگنال به چند سیگنال را نیز دارا می باشند. اما شما باید مراقب عملکرد انجام کار آنها باشید. اگر هر دو آنها اعمال یکسانی را انجام می دهند پس در چه مواردی متفاوت هستند؟

۶-۵-۱۰- هاب چیست؟

هاب در مدل OSI در لایه فیزیکی عمل می کند. از طرف دیگر، سوئیچ قدری هوشمند تر بوده و در مدل OSI در لایه انتقال داده (Data Link) عمل می کند.



زمانی که هاب از یک پورت اطلاعاتی را دریافت می کند، آن اطلاعات را به همه پورت ها پخش می کند. این عملکرد در هاب باعث هدر رفتن پهنای باند و ایجاد تداخل می شود.
تصور کنید که دو کامپیوتر به صورت همزمان اقدام به ارسال اطلاعات کنند، بسته های اطلاعات با یکدیگر برخورد کرده و در اثر این تداخل، اطلاعات دچار مشکل می شوند. در این شرایط ما مجبور به دوباره تکرار کردن اطلاعات از طریق فرآیند CSMA/CD که مخفف Carrier Sense Multiple Access / Collision Detection می باشد هستیم. به عبارت ساده تر، این فرآیند یک پروتکل می باشد که ما با استفاده از آن داده را دوباره ارسال می کنیم، قبل از اینکه تداخل رخ دهد.
تداخل ها معمولاً مسئله ای در هاب ها می باشند. اما مسئله مهمتر این است که هاب ها پهنای باند را نیز هدر می دهند. هاب ها به صورت یکطرفه عمل می کنند، بدین معنی که در یک زمان اطلاعات فقط می توانند در یک مسیر حرکت کنند. از آنجایی که ما به صورت یکطرفه عمل می کنیم، پهنای باند باید بین هر پورت در هاب تقسیم بندی شود. تصور کنید که شما

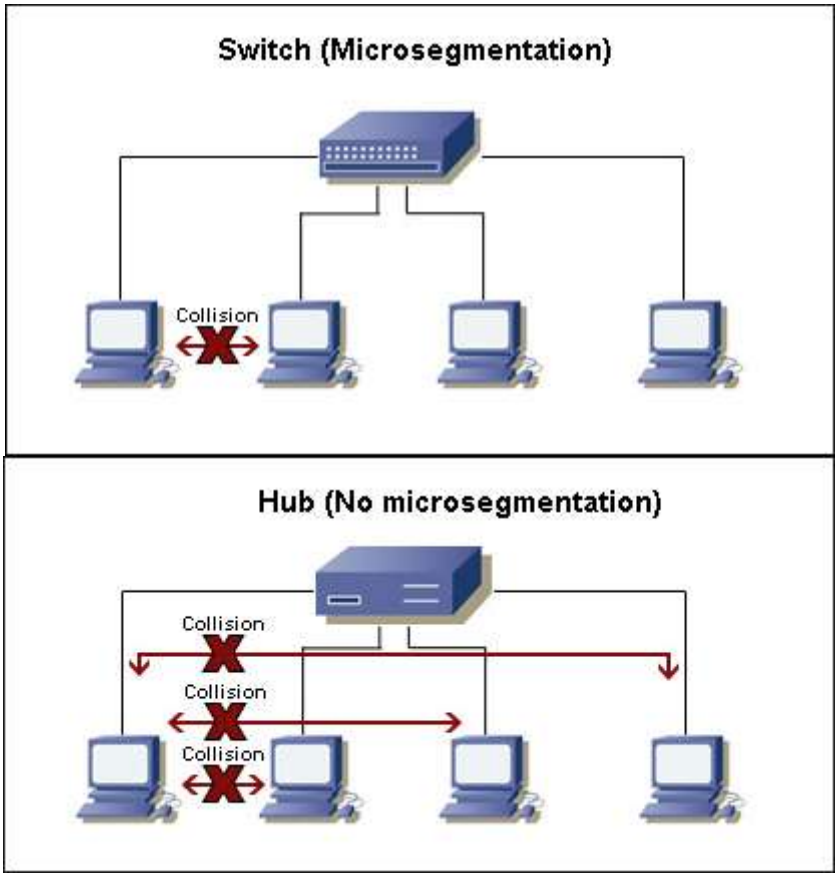
یک هاب ۲۰ پورت و یک سرعت ۲۰ کیلوبیت در ثانیه داریم. جالب است، اما شما فقط می توانید به هر کامپیوتر در شبکه ۱ کیلوبیت در ثانیه اختصاص دهید.

۶-۵-۱۱- سوئیچ چیست؟

در مدل OSI، سوئیچ در لایه انتقال داده (Data Link) عمل می کند. این بدان معنی است که سوئیچ هوشمند تر از هاب می باشد، بطوریکه سوئیچ در یک سطح پویا داده ها را مسیر دهی نماید. اگر اطلاعات بطور مثال مقصد معینی برای کامپیوتر A دارند سوئیچ فقط اطلاعات را به سمت کامپیوتر A مسیر دهی می کند.

برای جلوگیری از برخورد و تداخل آدرس دهی، سوئیچ ها از Micro Segmentation استفاده می کنند. Micro Segmentation اجازه ی تقسیم بندی دامنه های تداخل می دهد.

اجازه بدهید مثالی بزنیم، در شکل زیر، دامنه های تداخل بسیاری برای سوئیچ وجود دارند. برای نمونه اگر کامپیوتر های A و B در یک زمان با هم اقدام به ارسال اطلاعات نمایند، ممکن است تداخل به وجود آید. کامپیوتر A با کامپیوتر C یا کامپیوتر D، به هرحال هیچکدام فرآیند تداخل را تجربه نمی کنند. در یک شبکه مجهز به هاب، فقط یک دامنه تداخل وجود دارد. بدین معنی که اگر کامپیوتر اول بخواهد داده انتقال دهد، آن می تواند به صورت فاصله دار این کار را نسبت به کامپیوتر های دیگر شبکه انجام دهد.



سوئیچ می تواند آدرس یک کامپیوتر مورد پردازش قرار دهد که آیا یک پورت معین می باشد. اگر مقصد اطلاعات به سمت کامپیوتر A می باشد، اطلاعات فقط از طریق پورت کامپیوتر A انتقال داده می شود. بخاطر دارید که هاب چگونه پهنای باند را بین هر پورت تقسیم می کرد؟ تکنولوژی Micro Segmentation به ما این اجازه را می دهد که پهنای باند را برای هر کامپیوتر در بالاترین حد ممکن قرار دهیم. اگر 20 kb/s سرعت داریم هر کامپیوتر می تواند تمام 20 Kb/s را به خود اختصاص می دهد. (توجه داشته باشید که سوئیچ جادوگری نمی کند، اگر دو یا چند کامپیوتر در یک زمان در خط هستند، باید پهنای باند بین آنها تقسیم شود. در حال حاضر این تکنولوژی بهتر از هاب می باشد، به این دلیل که زمانیکه کامپیوتر در خط نیست پهنای باند به صورت اتوماتیک در خط تقسیم می شود.)

۶-۵-۱۲- آیا باید ما از هاب به سوئیچ ارتقاء پیدا کنیم؟

جواب این سوال قطعی است. بله. هاب ها ارزان تر و نصب آنها نیز ساده تر می باشد. اما عملکرد مناسبی ندارند و پهنای باند را نیز هدر می دهند. سوئیچ ها مقداری گرانتر هستند، و پیکربندی آنها گزینه های زیادی دارد، اما عملکرد آنها در شبکه بسیار بهتر و کارآمدتر می باشد.

۶-۶- پل (Bridge)

پل وسیله ای است که دو شبکه محلی را بدون توجه به اینکه از پروتکل یا ساختار یکسان استفاده می کنند یا خیر به یکدیگر متصل می کند و امکان جریان یافتن اطلاعات در بین آنها را فراهم می آورد.

به عبارت دیگر Bridge، سخت افزاری است که پل ارتباطی دو LAN مختلف می باشد. تفاوت بین یک پل یا Bridge و Router در تکنیک برقراری ارتباط بین دو LAN در این است که Router در هر شبکه ای عمل مسیر یابی را انجام می دهد و بر اساس IP مبدا و مقصد اطلاعات را در شبکه انتقال می دهد. اما یک Bridge که معمولاً در شبکه های مخابراتی و بی سیم بکار می رود، سخت افزار یا نرم افزاری است که اطلاعات از جنس لایه دوم یک شبکه (Frame) را در شبکه دیگر کپی می کند؛ به عنوان مثال دو LAN می توانند به وسیله خط تلفن به یک دیگر متصل شوند. استفاده از Bridge کارایی شبکه را تا حد زیادی کاهش می دهد و باعث کندی شبکه می شود. پل ها اصولا در شبکه هایی استفاده می شوند که از پروتکل های غیر قابل مسیر دهی استفاده می کنند. یعنی آدرس مبدا و مقصد ندارند. این پروتکل ها به راحتی از Bridge عبور می کنند. نمونه ای از این پروتکل ها NetBIOS و NetBeui می باشند.

توجه داشته باشید که با تقسیم یک شبکه ی بزرگ به چندین سگمنت و استفاده از یک پل برای اتصال آنها به یکدیگر، توان عملیاتی شبکه افزایش خواهد یافت. اگر یک سگمنت شبکه از کار بیفتد، سایر سگمنت ها ی متصل به پل می توانند شبکه را فعال نگه دارند. پل ها موجب افزایش وسعت شبکه محلی می شوند.

همانطور که می دانید، Repeater و هاب چنان طراحی شده اند که همه بار شبکه را که دریافت کرده اند به همه پورت های متصل به آنها، توزیع می نمایند. به عبارت دیگر ترافیک ایجاد شده در قسمتی از شبکه را به بخشهای دیگر شبکه عمومیت می دهند. به منظور رفع این مشکل از پل (Bridge) استفاده می کنند.

فرض کنید ۸ کامپیوتر را توسط ۲ تا هاب ۵ پورت به یکدیگر متصل کرده ایم. در این مثال، اگر اتصال هاب ها را به طور مستقیم به یکدیگر وصل کنیم، این امر باعث می شود که ترافیک هر بخش از شبکه، از هاب مربوطه رد شده و به هاب دیگر رسیده و از طریق آن، بخش دیگر شبکه را نیز تحت تاثیر خود قرار دهد. به این ترتیب ترافیک شبکه سیر صعودی خواهد داشت. برای رفع این مشکل از Bridge (پل) در نقطه میانی دو هاب استفاده می شود تا ترافیک در هر بخش، محلی باقی بماند و به بخش دیگر منتقل نشود و به این ترتیب ترافیک شبکه کاهش می یابد.

پل، این عملیات را توسط فیلتر کردن داده ها انجام می دهد. نحوه کار به این ترتیب است که پل آدرس فیزیکی تمام کامپیوتر های موجود در یک بخش را می داند و موقعیت آنها را در یک جدول داخل خود ذخیره می کند. وقتی که یک فریم از یک بخش وارد آن می شود، در جدول داخلی خود به دنبال آدرس فیزیکی آن می گردد تا آدرس مقصد فریم را مشخص کند.

اگر آدرس مقصد فریم در همان سگمنت آدرس مبدا باشد، پل از عبور فریم به بخشهای دیگر ممانعت به عمل آورده و فریم مربوطه در همان بخش به دنبال مقصد خود می گردد. ولیکن اگر فریم به سگمنت دیگری تعلق داشته باشد، پل فریم مربوطه

را به آن بخش پاس می دهد. به عبارت دیگر پل، فریم هایی را که آدرس مبدا و مقصدشان در یک بخش از شبکه است، در همان بخش نگه می دارد و با این کار باعث می شود ترافیک یک قسمت از شبکه به قسمت دیگر منتقل نشود.

به یاد داشته باشید که Bridge در لایه ۲ کار می کند و مفهوم MAC Address را از روی بسته ها می تواند بخواند و طبق جدول MAC Address ها، عمل فیلتر فریم ها را انجام می دهد.

همچنین Bridge می تواند شبکه های با رسانه های مختلف را به هم متصل کند. به عنوان مثال یک Bridge می تواند یک شبکه مبتنی بر فیبر نوری (100BaseFX) را به یک شبکه مبتنی بر کابل UTP (10BaseTX) متصل کند و کامپیوتر های موجود در بخشهای با رسانه ها و توپولوژی های متفاوت با یکدیگر به نقل و انتقالات داده بپردازند.

۶-۷- دروازه (Gateway)

Gateway یا مترجم پروتکل: وسیله ای است که معمولاً مانند یک دروازه ورودی/خروجی در شبکه عمل می کند. لفظ Gateway برای هر سخت افزاری به کار می رود که معمولاً دو شبکه غیر همجنس را به هم متصل کند. یک Gateway می تواند یک کامپیوتر، یک مسیریاب، یک Firewall، یک Proxy Server و یا هر چیز دیگری باشد. اما تجهیزاتی که خاص Gateway هستند معمولاً در شبکه هایی بکار می روند که براساس پروتکل TCP/IP کار نمی کنند. این تجهیزات وظیفه ترجمه پروتکل بین دو شبکه غیر همجنس را انجام می دهند. به عنوان مثال در شبکه هایی که TCP/IP Base نیستند، با استفاده از یک Gateway می توان پروتکل شبکه را به پروتکل TCP/IP و برعکس تبدیل نمود. یک کاربرد دیگر Gateway این است که می توان تنظیم نمود که تمامی Packet های خروجی یک کامپیوتر به سمت کامپیوتری خاص برود. مثلاً کامپیوتر سرویس دهنده اینترنت.

۶-۸- مسیریاب (Router)

مسیریاب و یا همان روتر، یک وسیله میانجی در شبکه های ارتباطی است که مسئولیت تحویل پیام ها را بر عهده دارد. در شبکه ای که کامپیوتر های زیادی را از طریق حلقه ای از اتصالات با یکدیگر مرتبط می کند، مسیریاب پیام های مورد نظر را هدایت می کند.

مسیریاب ها در مقایسه با هاب ها و سوئیچ ها، از هوشمندی بیشتری برخوردارند. مسیریاب ها از بسته، اطلاعات کاملتری جهت تشخیص این مسئله که کدام مسیریاب یا ایستگاه کاری، می بایست بسته بعدی را دریافت کند، دارا می باشد. مسیریاب ها از طریق نقشه مسیر شبکه، تحت عنوان "جدول مسیر یابی"، ارسال بسته ها از طریق بهترین مسیر به مقصد را تضمین می کنند. در صورت قطع ارتباط بین دو مسیریاب، مسیریاب ارسال کننده، مسیر دیگری را جهت ادامه سیر و حرکت در نظر می گیرد. در ضمن مسیریاب می تواند بین شبکه هایی که به زبانهای مختلفی صحبت می کنند، یعنی دارای "پروتکل های" مختلفی می باشند، ارتباط برقرار کند. برخی از این پروتکلها عبارتند از: پروتکل اینترنت (IP)، تبادل بسته های اینترنتی (IPX) و Apple Talk.

مسیریاب ها به سبب برخورداری از هوش بیشتر، قادرند با اجتناب از ایجاد ترافیک در برخی بخشهای دستیابی شبکه، باعث تامین امنیتی بیشتر بشوند.

مسیریاب ها می توانند شبکه ها را به یک مکان منفرد یا مجموعه ای از ساختارها متصل کرده و سبب تامین رابط هایی برای اتصال LAN ها به WAN بشوند، درست مثل ارتباط شعبه های اداری به یکدیگر یا به اینترنت.

مسیریاب ها در لایه ۳ مدل مرجع OSI کار می کنند؛ یعنی هر مسیریاب بسته را شناخته و می تواند از روی Header بسته ها، مبدا و مقصد را تشخیص دهد. وقتی کامپیوتری در یک شبکه بسته ای را ارسال می کند که مقصد آن در شبکه محلی متصل به آن کامپیوتر موجود نیست، کامپیوتر آن بسته را تحویل Gateway می دهد تا از شبکه خارج شود. Gateway ها در شبکه معمولاً تجهیزاتی هستند که عمل مسیر یابی را نیز انجام می دهند. پس Router شبکه یا همان Gateway آدرس

مقصد بسته ها را با مسیرهای خود مقایسه می کند تا کوتاه ترین و بهترین مسیر را بین مبدا و مقصد انتخاب کنند و در صورت وجود مسیر، بسته به خروجی مورد نظر ارسال می شود و در صورت عدم وجود مسیر، برای مسیر یابی Router یا با مسیریاب های مجاور مشورت می نماید و یا بسته را تحویل مسیریاب بعدی که در واقع Gateway مربوط به این مسیریاب می باشد هدایت می کند. هر Router دارای یک Routing Table می باشد که این جدول به صورت پویا نسبت به مسیریاب های همسایه به روز رسانده می شود. (پروتکل هایی مانند RIP و OSPF). به عبارت بهتر مسیریاب ها همیشه در مورد مسیرهای موجود برروی اینترنت با یکدیگر تبادل نظر می نمایند. مسیریاب ها همواره به دنبال بهترین مسیر با کمترین هزینه برروی اینترنت می گردند.

۶-۸-۱- آشنائی با روتر

استفاده از روتر ها 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 های از راه دور) در عصر حاضر است. نام در نظر گرفته شده برای روتر ها، متناسب با کاری است که آنان انجام می دهند: "ارسال و مسیر دهی داده از یک شبکه به شبکه ای دیگر". مثلاً در صورتی که یک شرکت دارای شعبه ای در اصفهان و یک دفتر دیگر در شیراز باشد، به منظور اتصال آنان به یکدیگر می توان از یک خط Leased (اختصاصی) که به هر یک از روتر های 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 غیر ضروری دیگر فیلتر و در پهنای باند و هزینه های مربوطه، صرفه جویی می گردد.

۶-۸-۲- انواع روتر

روتر ها را می توان به دو گروه عمده سخت افزاری و نرم افزاری تقسیم نمود:

روتر های سخت افزاری: روتر های فوق، سخت افزارهایی می باشند که نرم افزارهای خاص تولید شده توسط تولیدکنندگان را اجراء می نمایند (در حال حاضر صرفاً به صورت Black Box (جعبه سیاه) به آنان نگاه می کنیم). نرم افزار فوق، قابلیت مسیر دهی را برای روتر ها فراهم نموده تا آنان مهمترین و شاید ساده ترین وظیفه خود که ارسال داده از یک شبکه به شبکه دیگر است را به خوبی انجام دهند. اکثر شرکت ها ترجیح می دهند که از روتر های سخت افزاری استفاده نمایند، چراکه آنان در مقایسه با روتر های نرم افزاری، دارای سرعت و اعتماد پذیری بیشتری می باشند. شکل زیر یک نمونه روتر را نشان می دهد.

روتر های نرم افزاری: روتر های نرم افزاری دارای عملکردی مشابه با روتر های 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 ویندوز سرور، یک سرویس دهنده Novell Netware و یا یک سرویس دهنده لینوکس باشد. تمامی سیستم های عامل شبکه ای مطرح، دارای قابلیت های مسیر دهی از قبل تعبیه شده می باشند.

در اکثر موارد از روتر ها به عنوان فایروال و یا Gateway اینترنت، استفاده می گردد. در این رابطه لازم است به یکی از مهمترین تفاوت های موجود بین روتر های نرم افزاری و سخت افزاری، اشاره گردد: در اکثر موارد نمی توان یک روتر نرم افزاری را جایگزین یک روتر سخت افزاری نمود، چراکه روتر های سخت افزاری دارای سخت افزار لازم و از قبل تعبیه شده ای می باشند که به آنان امکان اتصال به یک لینک خاص WAN (از نوع Frame Relay، ISDN و یا ATM) را خواهد داد. یک

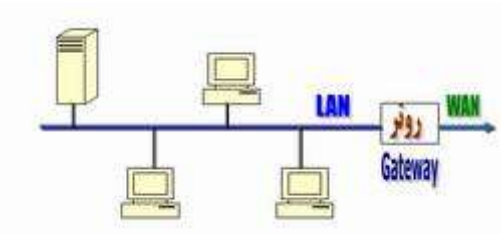
روتر نرم افزاری (نظیر سرویس دهنده ویندوز) دارای تعدادی کارت شبکه است که هر یک از آنان به یک شبکه LAN متصل شده و سایر اتصالات به شبکه های WAN از طریق روتر های سخت افزاری، انجام خواهد شد.

مثال ۱: استفاده از روتر به منظور اتصال دو شبکه به یکدیگر و ارتباط به اینترنت

فرض کنید از یک روتر مطابق شکل زیر به منظور اتصال دو شبکه LAN به یکدیگر و اینترنت، استفاده شده است. زمانی که روتر داده ای را از طریق یک شبکه LAN و یا اینترنت دریافت می نماید، پس از بررسی آدرس مبداء و مقصد، داده دریافتی را برای هر یک از شبکه ها و یا اینترنت ارسال می نماید. روتر استفاده شده در شکل زیر، شبکه را به دو بخش متفاوت تقسیم نموده است (دو شبکه مجزا). هر شبکه دارای یک هاب است که تمامی کامپیوتر های موجود در شبکه به آن متصل شده اند. علاوه بر موارد فوق، روتر استفاده شده دارای اینترفیس های لازم به منظور اتصال هر شبکه به آن بوده و از یک اینترفیس دیگر به منظور اتصال به اینترنت، استفاده می نماید. بدین ترتیب، روتر قادر است داده مورد نظر را به مقصد درست، ارسال نماید.

مثال ۲: استفاده از روتر در یک شبکه LAN

فرض کنید از یک روتر مطابق شکل زیر در یک شبکه LAN، استفاده شده است. در مدل فوق، هر یک از دستگاههای موجود در شبکه با روتر موجود نظیر یک Gateway برخورد می نمایند. بدین ترتیب، هر یک از ماشین های موجود بر روی شبکه LAN که قصد ارسال یک بسته اطلاعاتی (اینترنت و یا هر محل خارج از شبکه LAN) را داشته باشند، بسته اطلاعاتی موردنظر را برای Gateway ارسال می نمایند. روتر (Gateway) نسبت به محل ارسال داده دارای آگاهی لازم می باشد (در زمان تنظیم خصلت های پروتکل TCP/IP برای هر یک از ماشین های موجود در شبکه یک آدرس IP برای Gateway در نظر گرفته می شود). شکل زیر نحوه استفاده از یک روتر به منظور دستیابی کاربران به اینترنت در شبکه LAN را نشان می دهد:



مثال ۳: استفاده از روتر به منظور اتصال دو دفتر کار

فرض کنید، بخواهیم از روتر به منظور اتصال دو دفتر کار یک سازمان به یکدیگر، استفاده نماییم. بدین منظور هر یک از روتر های موجود در شبکه با استفاده از یک پروتکل WAN نظیر ISDN به یکدیگر متصل می گردند. عملاً، با استفاده از یک کابل که توسط ISP مربوطه ارائه می گردد، امکان اتصال به اینترفیس WAN روتر فراهم شده و از آنجا سیگنال مستقیماً به شبکه ISP مربوطه رفته و سر دیگر آن به اینترفیس WAN روتر دیگر متصل می گردد. روتر ها، قادر به حمایت از پروتکل های WAN متعددی نظیر Frame Relay , ATM , HDLC و یا PPP، می باشند.

۶-۸-۳- مهمترین ویژگی های یک روتر

روتر ها دستگاههای لایه سوم (مدل مرجع OSI) می باشند.

روتر ها مادامی که برنامه ریزی نگردند، امکان توزیع داده را نخواهند داشت.

اکثر روتر های مهم دارای سیستم عامل اختصاصی خاص خود می باشند.

روتر ها از پروتکل های خاصی برای مبادله اطلاعات ضروری خود (منظور داده نیست)، استفاده می کنند.

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

۶-۸-۴- آشنائی با اینترفیس های (رابط) روتر

اینترفیس ها مسئولیت اتصالات روتر به دنیای خارج را برعهده داشته و می توان آنان را به سه گروه عمده اینترفیس های مختص شبکه محلی، اینترفیس های مختص شبکه WAN و اینترفیس های کنسول و کمکی تقسیم نمود. در ادامه با اینترفیس های فوق آشنا خواهیم شد.

انواع اینترفیس های روتر

اینترفیس ها مسئولیت اتصالات روتر به دنیای خارج را برعهده داشته و می توان آنان را به سه گروه عمده تقسیم نمود:

۱- اینترفیس های مختص شبکه محلی: با استفاده از اینترفیس های فوق یک روتر می تواند به محیط انتقال شبکه محلی متصل گردد. اینگونه اینترفیس ها معمولاً نوع خاصی از اترنت می باشند. در برخی موارد ممکن است از سایر تکنولوژی های LAN نظیر Token Ring و یا ATM (برگرفته ازAsynchronous Transfer Mode) نیز استفاده گردد.

۲- اینترفیس های مختص شبکهWAN: این نوع اینترفیس ها اتصالات مورد نیاز از طریق یک ارائه دهنده سرویس به یک سایت خاص و یا اینترنت را فراهم می نمایند. اتصالات فوق ممکن است از نوع سریال و یا هر تعداد دیگر از اینترفیس های WAN باشند. در زمان استفاده از برخی اینترفیس هایWAN، به یک دستگاه خارجی نظیرCSU به منظور اتصال روتر به اتصال محلی ارائه دهنده سرویس نیاز می باشد. در برخی دیگر از اتصالاتWAN، ممکن است روتر مستقیماً به ارائه دهنده سرویس متصل گردد.

۳- اینترفیس های کنسول و کمکی: عملکرد پورت های مدیریتی متفاوت از سایر اتصالات است. اتصالات LAN وWAN، مسئولیت ایجاد اتصالات شبکه ای به منظور ارسال فریم ها را برعهده دارند ولی پورت های مدیریتی یک اتصال مبتنی بر متن به منظور پیکربندی و اشکال زدایی روتر را ارائه می نمایند. پورت های کمکی (Auxiliary) و کنسول (Console) دو نمونه متداول از پورت های مدیریت روتر می باشند. این نوع پورت ها، از نوع پورت های سریال غیر همزمان EIA-232 می باشند که به یک پورت ارتباطی کامپیوتر متصل می گردند. در چنین مواردی از یک برنامه شبیه ساز ترمینال بر روی کامپیوتر به منظور ایجاد یک ارتباط مبتنی بر متن با روتر استفاده می گردد. مدیران شبکه می توانند با استفاده از ارتباط ایجاد شده مدیریت و پیکربندی دستگاه مورد نظر را انجام دهند.

شکل زیر انواع اتصالات یک روتر را نشان می دهد.

۶-۸-۵- پیکربندی روتر با استفاده از پورت های مدیریت

پورت های کنسول و کمکی به منزله پورت های مدیریتی می باشند که از آنان به منظور مدیریت و پیکربندی روتر استفاده می گردد. این نوع پورت های سریال غیر همزمان به عنوان پورت های شبکه ای طراحی نشده اند. برای پیکربندی اولیه روتر از یکی از پورت های فوق استفاده می گردد. معمولاً برای پیکربندی اولیه، استفاده از پورت کنسول توصیه می گردد چراکه تمامی روتر ها ممکن است دارای یک پورت کمکی نباشند.

زمانی که روتر برای اولین مرتبه وارد مدار و یا سرویس می گردد، با توجه به عدم وجود پارامترهای پیکربندی شده، امکان برقراری ارتباط با هیچ شبکه ای وجود نخواهد داشت. برای پیکربندی و راه اندازی اولیه روتر، می توان از یک ترمینال و یا کامپیوتر که به پورت کنسول روتر متصل می گردد، استفاده نمود. پس از اتصال کامپیوتر به روتر، می توان با استفاده از دستورات پیکربندی، تنظیمات مربوطه را انجام داد. پس از پیکربندی روتر با استفاده از پورت کنسول و یا کمکی، زمینه اتصال روتر به شبکه به منظور اشکال زدایی و یا مانیتورینگ فراهم می گردد.

نحوه اتصال به پورت کنسول روتر

برای اتصال کامپیوتر به پورت کنسول روتر به یک کابل Rollover و یک آداپتور RJ-45 to DB-9 نیاز می باشد. روتر های سیسکو به همراه آداپتور های مورد نیاز برای اتصال به پورت کنسول ارائه می گردند. کامپیوتر و یا ترمینال می بایست قادر به حمایت از شبیه سازی ترمینال VT100 باشند. در این رابطه از نرم‌افزارهای شبیه‌ساز ترمینال نظیر HyperTerminal استفاده می گردد.

برای اتصال کامپیوتر به روتر می بایست مراحل زیر را دنبال نمود:

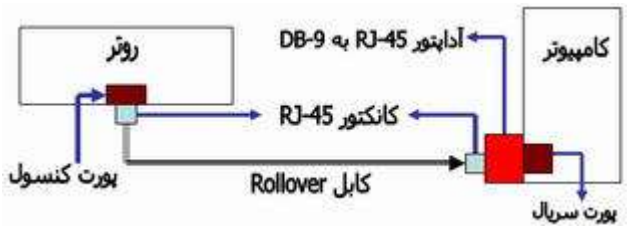
پیکربندی نرم افزار شبیه سازی ترمینال بر روی کامپیوتر انتخاب شماره پورت مناسب و...

اتصال کانکتور RJ-45 کابل rollover به پورت کنسول روتر

اتصال سر دیگر کابل rollover به آداپتور RJ-45 to DB-9

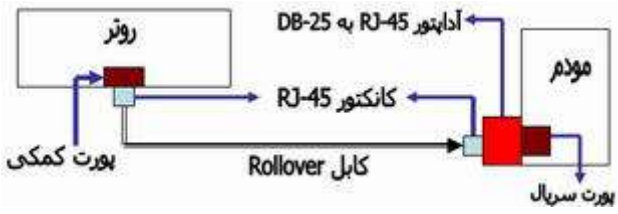
اتصال آداپتور DB-9 به کامپیوتر

شکل زیر نحوه اتصال کامپیوتر به روتر را با استفاده از یک کابل Rollover نشان می دهد:



اتصال کامپیوتر به روتر

برای مدیریت و پیکربندی از راه دور روتر، می توان یک مودم را به پورت کنسول و یا کمکی روتر متصل نمود. شکل زیر نحوه اتصال روتر به یک مودم را نشان می دهد:



ارتباط با روتر از طریق مودم

به منظور اشکال زدایی روتر، استفاده از پورت کنسول نسبت به پورت کمکی ترجیح داده می شود. در زمان استفاده از پورت کنسول به صورت پیش فرض پیام های خطا، اشکال زدایی و راه اندازی نمایش داده می شوند. از پورت کنسول در مواردی که

سرویس های شبکه فعال نشده و یا با مشکل مواجه شده اند نیز می توان استفاده نمود. بنابراین پورت کنسول گزینه ای مناسب برای بازیابی رمز عبور و سایر مشکلات غیرقابل پیش بینی می باشد.

اتصال اینترفیس های LAN

در اکثر محیط هایLAN، روتر با استفاده از یک اینترفیس Ethernet و یا Fast Ethernet به شبکه متصل می گردد. در چنین مواردی روتر همانند یک میزبان است که با شبکه LAN از طریق یک هاب و یا سوئیچ ارتباط برقرار می نماید.

به منظور ایجاد اتصال از یک کابل Straight-Through استفاده می گردد. در برخی موارد، اتصال اترنت روتر مستقیماً به کامپیوتر و یا روتر دیگری متصل می گردد. در چنین مواردی از یک کابل Cross-over استفاده می گردد. در صورت عدم استفاده صحیح از اینترفیس ها، ممکن است روتر و یا سایر تجهیزات شبکه ای با مشکل مواجه گردند.

اتصال اینترفیس های WAN

اتصالات WAN دارای انواع مختلفی بوده و از تکنولوژی های متفاوتی استفاده می نمایند. سرویس های WAN معمولاً از ارائه دهندگان سرویس اجاره می گردد. خطوط Leased و یا Packet-Switched نمونه هایی از انواع متفاوت اتصالات WAN می باشند.

برای هر یک از انواع سرویس هایWAN، دستگاه مشتری (اغلب یک روتر است) به منزله یک DTE (Data Terminal Equipment) رفتار می نماید. پایانه فوق با استفاده از یک دستگاه DCE (Data Circuit-Terminating Equipment) که معمولاً یک مودم و یا CSU/DSU (Channel Service Unit/Data Service Unit) می باشد به ارائه دهنده سرویس متصل می گردد.

از دستگاه فوق برای تبدیل داده از DTE به یک شکل قابل قبول برای ارائه دهنده سرویسWAN، استفاده می گردد.

۶-۸-۶- آشنایی با مسیریاب های سیسکو

تاریخچه مسیریاب های سخت افزاری

نام کلی که برای مسیریاب ها در نظر گرفته شده به خاطر اولین و اصلی ترین وظیفه هر روتر یعنی عمل مسیر یابی است و انتخاب این نام هم به سال ۱۹۸۴ بر می گردد. یعنی زمانی که رفته رفته با ظهور کامپیوتر های شخصی مشکل تعدد استانداردها تبدیل به یک مشکل حاد برای شبکه های موجود شد. گویا در این هنگام دو دانشمند به نام های Leonard Bosack و Sandy Lerner از دانشگاه استنفورد برای اتصال شبکه ها و مسیر یابی داده ها بین این شبکه ها و حل مشکل عدم سازگاری پروتکل های مختلف در سطح مسیریاب ها، ایده مسیر یابی (Routing) را مطرح نمودند و موفق شدند اولین مسیریاب را با هزینه شخصی تولید کرده و آن را در دانشگاه استنفورد نصب نمایند. با توجه به استقبالی که از این محصول جدید شد این دو نفر تصمیم گرفتند که محصول خود را تجاری کنند. در این سال بود که غول تجهیزات شبکه های کامپیوتری یعنی شرکت سیسکو در زمینه طراحی و تولید مسیریاب های سخت افزاری حرف اول را زد و در این زمینه به جز چند شرکت ازجمله Foundry Networks و Nortel Networks رقیب جدی دیگری نداشت و طی سال ها با ارائه راه حل های جدیدی نظیر ایجاد تنوع در کلیه محصولات و ارائه گواهینامه های مهندسی تجهیزات سیسکو نظیر CCNA، CCDA، CCNP و CCIE و... موقعیت خود را بیش از پیش تثبیت نموده است. به همین دلیل از مجموعه شرکت های تولیدکننده روتر های سخت افزاری تنها برروی مسیریاب های شرکت سیسکو تمرکز می کنیم و به دلیل تنوع زیاد مسیریاب های این شرکت و

همچنین تعدد ماژول های مورد استفاده که به منظور افزایش انعطاف پذیری مسیریاب ها استفاده می شوند، تنها به تشریح مدل های معروف تر خواهیم پرداخت. یک مسیریاب صرف نظر از نوع، سری و قیمت آن، همانند یک کامپیوتر دارای اجزای سخت افزاری نظیر جعبه (Case) برد اصلی (Mother Board)، پردازنده، حافظه موقت (RAM)، حافظه دائمی (Flash) و رابط ها و ماژول های مختلف است که بسته به کاربرد هر مسیریاب توان و ظرفیت متفاوتی دارند و همچنین هر مسیریاب دارای یک سیستم عامل است که IOS نامیده می شود و سرنام کلمات Internetworking Operating System می باشد. ولی از آنجائی که مسیریاب ها فاقد صفحه کلید و مانیتور هستند، معمولاً به سه طریق می توان فرامین سیستم عامل را برای پیکربندی مسیریاب وارد نمود، این سه روش عبارتند از:

۱) کنسول

به همراه هر مسیریاب یک کابل ۸ رشته مخصوص به نام کابل Rollover ارائه می شود که با استفاده از آن و یک کامپیوتر شخصی و از طریق برنامه هایی نظیر Term90 یا HyperTerminal ویندوز که قابلیت تبادل داده با پورت های سریال کامپیوتر را دارند، می توان پیکربندی روتر را در بالاترین سطح دسترسی انجام داد.

کابل کنسول روتر

نکته:

- با امکان دسترسی فقط در این سطح، می توان تحت شرایطی حتی رمز های عبور دستگاه را نیز تعویض نمود. به همین دلیل است که حفاظت فیزیکی دستگاه روتر بسیار حائز اهمیت است.
- اولین باری که بخواهید پیکربندی یک روتر را انجام دهید، حتماً می بایست از این طریق اقدام کنید.

۲) Telnet

از آنجایی که اصولا مسیریاب ها در لایه شبکه مدل TCP/IP کار می کنند، می توانیم به آنها آدرس IP اختصاص دهیم و طبعاً با استفاده از پروتکل Telnet و پورت اترنت روتر می توانیم از راه دور به آن متصل شده و روتر را پیکربندی کنیم. البته باید بدانید که اجازه این نوع دسترسی قبلاً می بایست از طریق کنسول صادر شده باشد و همچنین این که کاربری که به این صورت به مسیریاب متصل شده، نسبت به روش اول از سطح دسترسی کمتری برخوردار است.

۳) Aux

این امکان برای مدیرانی است که می خواهند از طریق شماره گیری به مودم مسیریاب متصل شوند و آن را متناسب شرایط مد نظرشان پیکربندی کنند. برای این کار نیز لازم است از طریق کنسول دستگاه امکان استفاده از Aux را فعال نماییم.

در ادامه ابتدا در خصوص سری ها و مدل های مختلف مسیریاب های سیسکو و سپس درباره مشخصه های سخت افزاری مسیریاب ها و انواع آن ها نکاتی را عنوان می نماییم.

مشخصه های سخت افزاری مسیریاب های سیسکو

• Case

روتر های سیسکو با توجه به نوع و مدل دارای بدنه های متفاوتی هستند. مثلاً بدنه های Desktop که مربوط به سری های ۷۰ یا ۹۰ می باشند. این بدنه ها قابلیت افزودن ماژول یا سایر ملحقات را ندارند. در مقابل بدنه های Rackmount هستند که قابلیت نصب در رک را دارند. از همین نوع بدنه، بعضی که بزرگتر بوده و قابلیت نصب ماژول ها و کارت های زیادی به نام شاسی (Chasis) دارند شناخته میشوند.

• CPU

اگر بخواهید سرعت پردازنده های کامپیوتر های شخصی را با مسیریاب ها مقایسه کنید حتماً تعجب خواهید کرد، چرا که حتی سریع ترین روتر ها که می توانند در ستون فقرات شبکه های اینترنتی استفاده شوند و طبعاً می بایست حجم بسیار وسیعی از ترافیک اینترنت را در زمان بسیار کوتاهی پردازش نمایند، سرعتی در حدود ۲۰۰ مگاهرتز دارند. ولیکن از آنجایی که مسیریاب ها واسط گرافیکی کاربر ندارند و در محیط متنی کار می کنند و همچنین به دلیل تک منظوره بودن این پردازنده ها این سرعت برای این منظور کفایت خواهد کرد. ضمناً جالب است که بدانید مسیریاب های سیسکو عمدتاً از پردازنده های سری ۶۸۰۰۰ شرکت موتورولا استفاده می کنند.

• مادربورد

مادربورد های مورد استفاده شرکت سیسکو عمدتا توسط شرکت های Asus و Iwill و Supermicro ساخته می شوند و طبیعتاً برای سری های مختلف توان و مشخصه های متفاوتی ارائه می شود.

• حافظه

در سخت افزار مسیریاب های سیسکو بسته به نوع و کاربرد، از انواع مختلفی از حافظه ها پشتیبانی می شود که عبارتند از:

۱. **RAM** که گاهی DRAM نیز نامیده می شود و برای ذخیره اطلاعات حین کار به کار می رود و یا به اصلاح سیسکو برای نگهداری Running Config مورد استفاده قرار می گیرد.

در بعضی مدل ها، این حافظه قابل ارتقاء و در برخی دیگر ثابت می باشد و عموماً در ظرفیت های ۴ و ۸ و ۱۶ و ۳۲ و ۶۴ مگابایت موجود می باشد.

۲. **ROM**: که در این نوع حافظه یک تصویر قابل بوت از سیستم عامل روتر (IOS Image) قرار می گیرد و در مراحل اولیه روند بوت مسیریاب مورد استفاده قرار می گیرد.

۳. **Flash Memory**: همانند هارد دیسک در PC ها می باشد و برای ذخیره کل IOS مورد استفاده قرار می گیرد. ضمناً برای ذخیره فایل های پیکربندی نیز از این حافظه استفاده می شود که در ظرفیت های مختلفی عرضه می شود. البته نسبت به مدل و سری مسیریاب معمولاً قابل ارتقا است.

۴. **NVRAM**: روتر ها از فایلی به نام Startup Config برای نگهداری تنظیمات ابتدایی پیکربندی مسیریاب استفاده می کنند و این فایل در این حافظه نگهداری می شود و پس از این که در روند بوت به داخل RAM دستگاه روتر بارگذاری شد، Running Config نامیده می شود.

• Interface

لینک های هر مسیریاب برای ارتباط با دنیای خارج در قالب پورت ها و ماژول ها که برای انعطاف پذیری روتر ها در جهت انجام وظایف گوناگون قابل استفاده و تغییر است و داخل اسلات های توسعه قرار می گیرند. به عنوان مثال می توان یک ISP را در نظر گرفت که پس افزایش خطوط تلفن خود قادر خواهد بود ماژولی به نام AM (که شامل تعدادی مودم است) را به

اسلات روتر خود (روتری که در نقش یک Access Server عمل می کند) متصل کند و کارآیی روتر را افزایش دهد. البته به شرط این که آن روتر خاص امکان این گسترش را داشته باشد. برای آگاهی از امکانات هر مسیریاب و بررسی قابل گسترش بودن آن و نوع ماژول هایی که می توانید به آن متصل کنید، می بایست به راهنمای فنی هر مسیریاب یا سایت وب شرکت سیسکو (www.Cisco.Com) مراجعه کنید، مطمئنا در این سایت اطلاعات بسیار مفیدی خواهید یافت.

۶-۸-۷- BRouter

این وسیله ترکیبی از پل و مسیر یاب می باشد (BRIDGT+ROUTER). بسته های محلی می توانند از یک طرف شبکه به طرف دیگر با توجه به آدرس مقصد هدایت شوند؛ حتی اگر از هیچ پروتکل ارسالی هم پیروی نکنند. بسته هایی که دارای پروتکل مناسب هستند میتواند طبق مسیر خود به دنیای خارج از شبکه محلی فرستاده شوند. این دستگاه جزء قطعات بسیار گران قیمت شبکه محسوب می شوند که می توانند با توجه به پروتکلی که در شبکه پیاده سازی شده است. عمل پل و یا عمل روتر را انجام دهند.

BRouter میتواند دو دسته از ترافیک شبکه را مدیریت کند. (Bridged Traffic) و (Router Traffic)

۱. **در Bridge Traffic**، BRouter ترافیک شبکه را به همان روش Bridge مدیریت میکند یعنی در لایه ۲ عمل کرده و داده ها را بر اساس آدرس فیزیکی آنها فیلتر میکند و یا از خود عبور میدهد.
۲. **در Router Traffic**، BRouter می تواند بخش های مختلف شبکه با توپولوژی های متفاوت به هم وصل کند و عمل فیلتر داده ها را با توجه به آدرس منطقی آنها انجام دهد.

به عنوان مثال. یک BRouter میتواند به گونه ای پیکربندی شود که بخشی از شبکه با پروتکل NetBEUI را پل کند و بخش دیگر شبکه با توپولوژی TCP/IP را مسیر یابی کند.

فصل ۷

معماری شبکه

در فصل های گذشته با انواع توپولوژی ها، رسانه ها و ادوات اتصال به شبکه آشنا شدید. در این فصل قصد داریم به معرفی معماری های مختلف شبکه بپردازیم:

معماری یک شبکه بیانگر استانداردهای تعریف شده در خصوص نحوه اتصال کامپیوتر ها با یکدیگر و نحوه ارسال اطلاعات می باشد. به عبارت دیگر، **معماری شبکه مجموعه ای از استاندارد هایی است که نوع کابل کشی، اتصالات، توپولوژی، نحوه دسترسی به خطوط انتقال و سرعت انتقال را مشخص می کند.** بنابراین هنگام راه اندازی یک شبکه، باید ابتدا معماری شبکه مشخص شود و سپس با توجه به استاندارد هایی که معماری شبکه مشخص میکند، قطعات و اتصالات شبکه خریداری و پیکربندی گردد.

۷-۱- انواع معماری شبکه

- اترنت (Ethernet)
- Token Ring
- FDDI
- Wireless

۷-۱-۱- اترنت

اترنت متداولترین معماری شبکه است که با استفاده از مجموعه ای از قوانین و استاندارد ها، پیکربندی بستر شبکه و بالطبع نقل و انتقال داده ها در شبکه را قانونمند می کند. به عبارت دیگر با ارائه یکسری از استانداردها و یکسری محدودیت ها در بکارگیری تجهیزات، اتصالات، پهنای باند و.... تمام اجزای شبکه را با هم همزمان میکند.

قوانین نامگذاری اترنت توسط مؤسسه IEEE:

مؤسسه IEEE که یکی از مؤسسات بزرگ در خصوص استاندارد سازی تجهیزات و تکنولوژی ها است، استانداردهای شبکه را با روش 802.X نامگذاری می کند. به عنوان مثال این مؤسسه برای معماری شبکه اترنت، استاندارد 802.3 را مشخص کرده است که تمام جزئیات مربوط به این معماری شبکه در متن این استاندارد آورده شده است.

اترنت اولین بار در سال ۱۹۷۰ و بر روی شبکه های محلی با تکنولوژی خطی تعریف شد و در سال ۱۹۹۵ مؤسسه IEEE این معماری را با استاندارد 802.3 معرفی کرد. و لیکن از آن زمان تا کنون این معماری توسعه یافته و شامل خانواده ای از تکنولوژی های دیگر شده است و قابلیت های زیادی به این معماری افزوده شده است. به همین ترتیب مؤسسه IEEE نیز ضمیمه های جدیدی را برای 802.3 ارائه کرده است که این ضمیمه ها به صورت یک یا دو حرف تکمیلی است که در انتهای این استاندارد قید می شود. (802.3U)

به عنوان مثال پهنای باند ارائه شده توسط اترنت در ابتدا ۱۰ مگابیت در ثانیه بود و برای کامپیوتر های شخصی دهه ۸۰ که دارای سرعت پائین بودند، کافی بنظر می آمد؛ ولی در اوایل سال ۱۹۹۰ که سرعت کامپیوتر های شخصی و اندازه فایل ها افزایش یافت، مشکل پائین بودن سرعت انتقال داده بهتر نمایان شد. اکثر مشکلات فوق به کم بودن پهنای باند موجود مربوط می گردید . در سال ۱۹۹۵ موسسه IEEE، استانداردی را برای اترنت با سرعت ۱۰۰ مگابیت در ثانیه معرفی نمود. این روال ادامه یافت و در سال های ۱۹۹۸ و ۱۹۹۹ استاندارد هایی برای گیگابیت نیز ارائه گردید.

تمامی استانداردهای ارائه شده با استاندارد اولیه اترنت سازگار می باشند. به عنوان مثال یک فریم اترنت می تواند از طریق یک کارت شبکه با کابل کواکسیال ۱۰ مگابیت در ثانیه از یک کامپیوتر شخصی خارج و بر روی یک لینک فیبر نوری اترنت ۱۰ گیگابیت در ثانیه ارسال و در انتها به یک کارت شبکه با سرعت ۱۰۰ مگابیت در ثانیه برسد. تا زمانی که بسته اطلاعاتی بر روی شبکه های اترنت باقی است در آن تغییری داده نخواهد شد. موضوع فوق وجود استعداد لازم برای رشد و گسترش اترنت را به خوبی نشان می دهد. بدین ترتیب امکان تغییر پهنای باند بدون ضرورت تغییر در تکنولوژی های اساسی اترنت همواره وجود خواهد داشت.

مفهوم پهنای باند (Band Width):

در سیستم های انتقال آنالوگ، پهنای باند به حد فاصل بین پایین ترین و بالاترین فرکانسی که یک رسانه میتواند از خود عبور دهد گفته می شود. (پهنای باند بر حسب فرکانس و با واحد هرتز بیان می شود) (300HZ - 3000HZ)

در سیستم های انتقال دیجیتال، پهنای باند به ظرفیت انتقال اطلاعات گفته می شود وبا واحد bps (بیت در ثانیه) سنجیده می شود. از عوامل موثر در پهنای باند: طول، قطر و جنس کابل است. پهنای باند با طول کابل نسبت معکوس و با قطر کابل نسبت مستقیم دارد. یعنی هرچه طول کابل بیشتر شود پهنای باند کمتر شود و هر چه قطر کابل بیشتر شود پهنای باند نیز بیشتر است.

برای انتقال اطلاعات میتوان به دو روش از پهنای باند استفاده کرد:

۱. **تک باند (Base Band)**
۲. **باند پهن (Band Broad)**

۱. در روش Base Band (تک باند) از تمام پهنای باند برای ارسال یا دریافت اطلاعات استفاده می شود. به این معنی که در روش تک باند رسانه در هر لحظه فقط میتواند یک سیگنال را از خود عبور دهد در نتیجه ارسال نوبتی می شود و اطلاعات پشت سر هم و به صورت سریال ارسال میشوند. این روش انتقال دلیل به وجود آمدن مفهوم بسته (Packet)است. در شبکه های محلی از این روش برای انتقال اطلاعات استفاده می شوند. بدین ترتیب که از دو رشته کابل استفاده می شود که یکی برای ارسال و دیگری دریافت اطلاعات را انجام میدهد. اطلاعات به صورت بسته های مشخص پشت سر هم قرار میگیرند و ارسال شده و دریافت میگردد. (تمام سیستم های انتقال دیجیتال از روش Base Band استفاده میکنند) (کابل هم محور UTP).

۲. در روش Band Broad (باند پهن)، یک رسانه (کابل) میتواند در آن واحد یک یا چند سیگنال را به طور همزمان عبور دهد. هر سیگنال به صورت جداگانه ارسال می شود و تداخل بین سیگنال هایی متفاوت به وجود نمی آید. از این روش در سیستم های انتقال آنالوگ استفاده می شود و رسانه می تواند در آن واحد سیگنالهای متفاوتی را با فرکانس های مختلف از خود عبور دهد. از این روش در شبکه تلویزیون های کابلی و شبکه های WAN استفاده میگردد. (کابل هم محور – فیبر نوری).

مفهوم سرعت انتقال اطلاعات:

مقدار اطلاعاتی که در واحد زمان توسط تجهیزات شبکه ارسال می شود گفته می شود (مثلاً کارت شبکه 100 Mbps). سرعت انتقال اطلاعات با پهنای باند رابطه مستقیم دارد. هر چه پهنای باند بیشتر شود سرعت انتقال اطلاعات نیز بیشتر می شود و بر عکس.

نکته: پهنای باند، ظرفیت انتقال یک رسانه یا یک کابل است. در صورتی که سرعت انتقال، سرعت ارسال اطلاعات در واحد زمان است.

تکنولوژی های مختلف اترنت:

همانطور که پیشتر نیز گفته شد. معماری شبکه اترنت برای اولین بار در سال ۱۹۷۰ مطرح شد و طی سالیان بعد این معماری و استانداردهای آن توسعه یافته و با نام های دیگری نامگذاری شدند. امروزه برای معماری اترنت، تکنولوژی مختلفی مطرح شده است:

- **10 BASE 2**
- **10 BASE 5**
- **10 BASE T**
- **10 BASE FL**
- **100 BASE X**
- **1000 BASE X**
- **1000 BASE T**

نکته: در استاندارد هایی که نام برده شد، عدد اول نمایانگر سرعت انتقال، عبارت BASE به معنای BASE BAND بودن توپولوژی مذکور و عبارت پس از ان نوع کابل را مشخص میکند.

(T: Twisted Pair ،F: Fiber Optic)

10 BASE 2

10 BASE 2 برای انتقال داده ها از کابل های کواکسیال THINNET استفاده میکند که مشخصات این کابل توضیح داده شد. کانکتور های این شبکه از نوع BNC بوده و دو سر کابل باید توسط TERMINATOR مسدود شود تا شبکه فعال شود. از مزایای 10 BASE 2، می توان نصب ساده و هزینه راه اندازی بسیار کم آن را نام برد. توپولوژی 10 BASE 2 همان توپولوژی خطی است.

قوانینی که در 10 BASE 2 باید رعایت شود. عبارتند از:

- حداقل طول کابلی که کامپیوتر را به هم متصل میکند نباید کمتر از ۰/۵ متر باشد.
- برای اتصال T_CONNECTOR به کامپیوتر نباید از کابل استفاده کرد و باید آن را مستقیماً به کامپیوتر متصل نمود.
- فاصله اولین و آخرین کامپیوتر در شبکه نباید بیش از ۱۸۵ متر باشد. این فاصله از روی اندازه کابل اندازه گیری می شود.
- با استفاده از هاب (REPEATER) میتوان حداکثر فاصله بین اولین و آخرین کامپیوتر را تا ۹۲۵ متر افزایش داد و کامپیوتر ها نباید خارج از این محدوده باشند.
- در فواصل بین هر دو REPEATER نمیتوان بیش از ۳۰ دستگاه کامپیوتر به شبکه متصل کرد.
- ابتدا و انتهای کابل باید با TERMINATOR مسدود شود. TERMINATOR شبکه 10BASE2 یک مقاومت ۵۰ اهمی است که سیگنالهای الکتریکی به وجود آمده در کابل شبکه را مصرف کرده و از باقی ماندن آن در شبکه جلوگیری میکند.

10 BASE 5

در 10 BASE 5 از کابل کواکسیال THICKNET برای اتصال کامپیوتر ها به یکدیگر استفاده می شود. هر کامپیوتر توسط یک کابل AUI یا DIX به یک عدد TRANSCEIVER که به کابل شبکه متصل شده است، وصل می شود و هر دو انتهای

کابل با TERMINATOR مسدود می شود. اولین مزیت 10BASE5 مسافت نسبتا زیادی است که تحت پوشش خود قرار میدهد. قوانینی که در مورد 10BASE 5 وجود دارد. عبارتند از:

- حداقل طول کابلی که برای اتصال دو کامپیوتر استفاده می شود ۲/۵ متر است.
- حداکثر طول کابل یا حداکثر فاصله بین اولین و آخرین کامپیوتر شبکه ۵۰۰ متر است.
- یکی از TERMINATOR. ها باید به زمین متصل شود.
- اندازه کابلی که کامپیوتر را با TRANSCEIVER متصل میکند. نباید بیشتر از ۵۰ متر باشد.

10 BASE T

برای راه اندازی شبکه 10 BASE T از کابل های Twisted Pair (زوج به هم تابیده) استفاده می شود که حداکثر سرعت آن 10 Mbps است. در این استاندارد هر کامپیوتری که می خواهد به شبکه متصل شود مستقیماً توسط یک کابل به هاب وصل شده و هاب، ارتباط کامپیوتر ها را برقرار میکند. اتصالات این توپولوژی از نوع RJ-45 میباشد. SEGMENTE های مختلف می توانند توسط کابل های کواکسیال یا فیبر نوری به یکدیگر متصل شوند. برخی از انواع دستگاههایی که می توانند جایگزین هاب شوند. هوشمند بوده و می توانند ترافیک شبکه را کنترل کرده و آن را کاهش دهند. از مشخصه های بارز این شبکه گران قیمت بودن هزینه راه اندازی و نصب آن است.

قوانین 10 BASE T عبارتند از:

- حداکثر تعداد کامپیوتری که این شبکه به هم متصل میکند. ۱۰۲۴ دستگاه کامپیوتر است.
- کابل ها باید از نوع زوج به هم تابیده CAT 3 و CAT4 و CAT 5 باشند (نوع کابل از نظر داشتن محافظ تفاوتی نمیکند. میتوان از هر دو کابل UTP یا STP استفاده کرد).
- حداکثر فاصله هر کامپیوتر تا هاب ۱۰۰ متر است.
- حداقل طول کابل (فاصله بین کامپیوتر تا هاب.) ۲/۵ متر است.

10 BASE FL

10 BASE FL یکی از خصوصیات شبکه اترنتی است که برای انتقال اطلاعات از فیبر نوری استفاده می کند. سرعت انتقال در این شبکه 10 MBPS است. مهمترین مزیت 10 BASE FL، مسافت زیادی است که تحت پوشش قرار میدهد. این مسافت ۲ کیلومتر است. از مزایای دیگر این شبکه این است که عوامل خارجی، تاثیری روی اطلاعات داخل فیبر ندارد. به عبارت دیگر. در فیبر نوری هم شنوایی وجود ندارد و اطلاعات سالم به مقصد میرسد.

دو استاندارد دیگر به نام های 10 Base FB و 10 Base FP نیز مورد استفاده قرار می گیرد. 10 Base FB یک شبکه اترنت همزمان است و برای اتصال دو تقویت کننده فیبر نوری به یکدیگر که در مسیر بین دو ایستگاه قرار دارد، استفاده می شود. استاندارد دیگر 10 Base FP است که یک شبکه ستاره ای با استفاده از فیبر نوری می باشد که برای Backbone شبکه ها مورد استفاده قرار می گیرد. در 10Base FP، نور به جای سیگنالهای الکترونیکی مسئولیت انتقال اطلاعات را برعهده دارد.

100Base X

ساختار شبکه 100 BASE X همانند شبکه 10 BASE T است. (سرعت این شبکه 100 MBPS است) با این تفاوت که 100 BAE X با سه مدل کابل کشی متفاوت مورد استفاده قرار می گیرد. این سه مدل عبارتند از:

- 100BASE TX: در این مدل از دو کابل CAT-5 از نوع UTP یا STP به صورت همزمان استفاده می شود.
- 100 BASE FX: در این مدل از دو رشته فیبر نوری در کنار هم استفاده می شود.
- 100 BASE T4: در این مدل ۴ رشته کابل Cat-5 یا Cat-3 در کنار هم استفاده می شود.

توجه: 100 BASE X با نام Fast Ethernet نیز شناخته می شود.

1000 BASE X

این استاندارد شبکه ای را توضیح میدهد که درآن سرعت انتقال اطلاعات یک گیگابایت در ثانیه است و برای انتقال اطلاعات از فیبر نوری استفاده می شود. این استاندارد خود از چند قسمت تشکیل شده است که عبارتند از:

۱. 1000 BASE SX
۲. 1000 BASE LX/LH
۳. 1000 BASE ZX

تفاوت استاندارد های ذکر شده در طول کابل و نوع فیبر نوری است که در آنها استفاده می شود.

1000 BASE T

در این استاندارد، از کابل های زوج به هم تابیده برای راه اندازی شبکه ای با سرعت یک گیگابیت در ثانیه استفاده می شود. این کابل ها از نوع CAT5 و کانکتورهای آن نیز از نوع RJ-45 است. نحوه ارسال اطلاعات در این استاندارد به گونه ای است که سیستم، توانایی انتقال اطلاعات با سرعت یک گیگابیت در ثانیه را پیدا میکند.

۷-۱-۳- TOKEN RING

شبکه Token Ring از نظر ظاهری یک شبکه ستاره ای است ولی به صورت Token Passing کار میکند. در این شبکه یک حلقه منطقی به وجود می آید و Token در امتداد حلقه حرکت کرده و به کامپیوتر ها میرسد. هر کامپیوتری که به ارسال اطلاعات نیاز داشته باشد. Token را نگه داشته و اطلاعات خود را به سوی مقصد ارسال میکند. اطلاعات ارسال شده در همان حلقه مجازی و در امتداد حرکت Token مسیر خود را طی میکند تا به کامپیوتر مقصد برسد. کامپیوتر مقصد در صورت صحیح بودن اطلاعات ارسالی، در جواب یک بسته به نام Acknowledge به کامپیوتر مبداء ارسال می کند. کامپیوتر مبداء نیز Token اصلی را از بین برده و یک Token جدید تولید می نماید و آن را در امتداد مسیر Token قبلی به حرکت در می آورد. این پروسه به همین صورت ادامه خواهد یافت.

در شبکه Token Ring در محل اتصال کامپیوتر ها به جای هاب از دستگاهی بنام MAU استفاده می شود. سرعت انتقال اطلاعات در این شبکه 16 Mbps یا 4 Mbps است. کارت های 16 Mbps می توانند با سرعت 4 Mbps نیز فعالیت کنند.

در شبکه Token Ring از کابل های زوج به هم تابیده استفاده می شود. اگر از کابل UTP در این توپولوژی استفاده شود، حداکثر طول کابل میتواند ۴۵ متر باشد و این شبکه فقط با سرعت ۴ مگابیت در ثانیه کار می کند و اگر از کابل STP استفاده شود. حداکثر طول کابل ۱۰۱ متر و با سرعت ۱۶ مگابیت در ثانیه اطلاعات منتقل می شود.

۷-۱-۴- FDDI

FDDI، تکنولوژی یک شبکه با سرعت ۱۰۰ مگابیت در ثانیه است که برای ارتباط از فیبر نوری استفاده میکند. در این تکنولوژی به جای فیبر نوری از کابل مسی نیز می توان استفاده کرد ولی در صورت استفاده از کابل مسی طول کابل کمتر می شود. FDDI به عنوان Backbone در محل هایی که تعداد زیادی کامپیوتر در آن قرار دارد، استفاده می شود. از جمله این محیط ها می توان به دانشگاه ها اشاره کرد. در FDDI میتوان ۵۰۰ گره را در مسافت ۱۰۰ کیلومتر به یکدیگر متصل کرد. توپولوژی فیزیکی این شبکه حلقوی است. نحوه به وجود آمدن این حلقه به این صورت است که یک حلقه ۱۰۰ کیلومتری از فیبر ساخته می شود و در هر ۲ کیلومتر یک تقویت کننده قرار میگیرد. برای جلوگیری از اختلالاتی که در اثر قطع شدن فیبر نوری به وجود می آید، از دو حلقه فیبر نوری در کنار هم استفاده می شود تا در صورتی که یکی از رشته ها قطع شود، رشته دوم وارد عمل شده و جایگزین رشته اول شود.

۷-۱-۵- شبکه بدون سیم

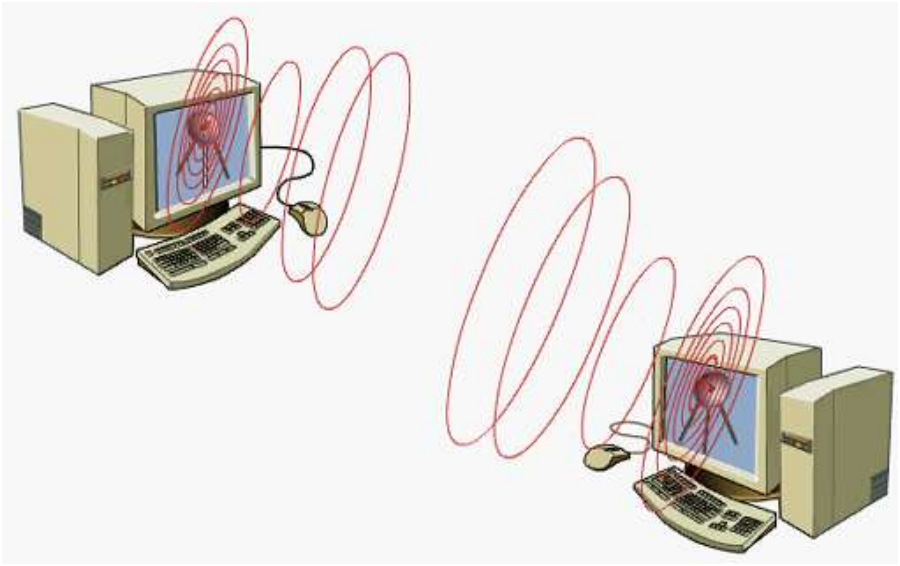
شبکه بدون سیم. شبکه ای است که از امواج رادیویی Broad Band برای مرتبط کردن کامپیوتر ها به یکدیگر استفاده می کند. از سیستم بیسیم معمولاً در شبکه های WAN استفاده می شود. کاربرد آن می تواند مرتبط کردن دو یا چند شبکه محلی، ارائه سرویس اینترنت و سرویس های دیگر باشد. شبکه بیسیم برای برقراری بین کامپیوتر هایی که نزدیک یکدیگر قرار دارند نیز استفاده می شود که در اینصورت نوعی شبکه به نام PAN بکار می رود.

در شبکه های PAN نیازی به استفاده از تجهیزات خاص شبکه نیست و فقط با نصب دو کارت شبکه PAN روی دو کامپیوتر که در فاصله مناسب از یکدیگر قرار گرفته اند، می توان یک شبکه را راه اندازی کرد. از مزایای شبکه های بیسیم این است که نیازی به نصب کابل شبکه و تجهیزات آن نیست و سرعت انتقال اطلاعات نیز می تواند تا سرعت ۵۲ مگابیت در ثانیه افزایش پیدا کند.

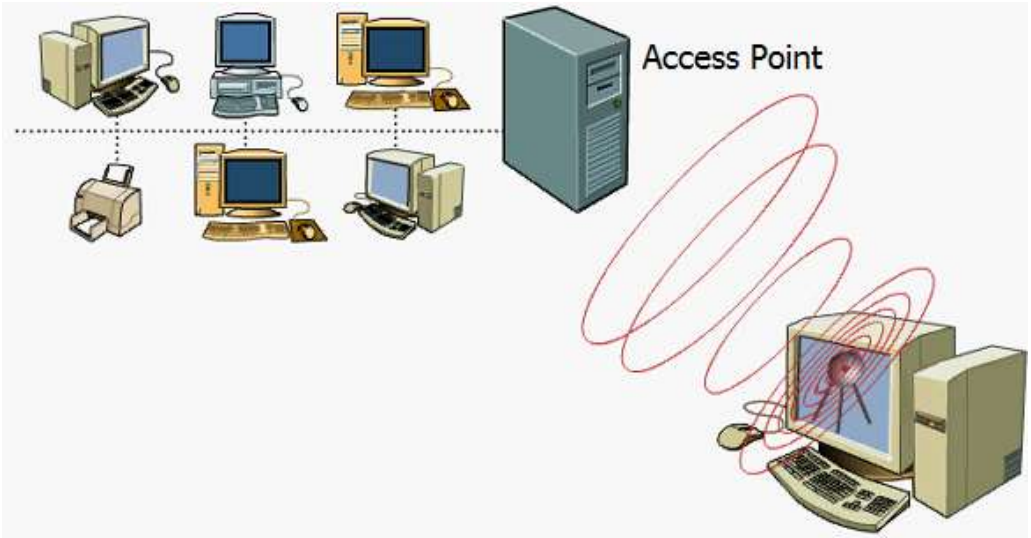
شبکه های بی سیم به ۲ طریق می توانند با یکدیگر ارتباط برقرار کنند.

۱- Ad hoc: در این روش، دو یا چند کامپیوتر توسط کارت شبکه بی سیم و به صورت مستقیم (Peer to Peer) به یکدیگر متصل می شوند. در این روش به هیچ عنصر سخت افزاری دیگری نیاز نمی باشد و همچنین الگوریتم مسیر یابی به صورت توزیع شده و توسط تمامی کامپیوتر ها انجام می گیرد. لذا می توان در حرکت از این نوع شبکه استفاده نمود و مثلاً هر کامپیوتر در یک اتومبیل جدا بوده و اتومبیل ها نیز در حال حرکت باشند.

به عبارت دیگر AD HOC استانداردی است که ارتباط بی سیم بین رایانه و تجهیزات جانبی مانند رایانه جیبی PDAs، تلفن همراه یا رایانه کیفی را برقرار می سازد.



۲- Infra-Structure: در این روش می توان کامپیوتری که کارت شبکه بیسیم دارد را به یک شبکه سیمی متصل نمود. بدین منظور کافی است که به یکی از سیستم های شبکه سیمی یک سخت افزار به نام Access Point یا به اختصار AP نصب کرد و از طریق آن با کامپیوتری که کارت شبکه بیسیم دارد ارتباط برقرار نمود. در این روش، بر عکس روش Ad Hoc، یک نقطه مرکزی وجود دارد که به عنوان محور بوده و به عنوان محل اتصال کامپیوتر ها شناخته می شود.



فصل ۸

OSI و TCP/IP

۸-۱- نحوه مبادله داده بین دو کامپیوتر

آیا تاکنون برای شما این سوال مطرح شده است که نحوه مبادله اطلاعات بین دو کامپیوتر موجود در یک شبکه به چه صورت است؟

در سالهای آغازین طراحی شبکه، مشکل عمده ای که وجود داشت نا سازگاری بین محصولات تولید شده توسط شرکت های بزرگ تولید کننده تجهیزات شبکه بود. این مشکل زمانی آغاز گردید که شرکت HP تصمیم به تولید یک محصول شبکه ای نمود و این محصول با محصولات مشابه سایر شرکت ها (مثلاً IBM) سازگار نبود. برای حل این مشکل نیاز به یک مدل مرجع برای تبادل اطلاعات در شبکه احساس می شد تا اینکه کمیته IEEE به منظور جلوگیری از عدم هماهنگی بین محصولات، پیشگام تعریف یک استاندارد برای محصولات شبکه شد و در سال ۱۹۸۴ مدل مرجع OSI را معرفی کرد. مدل فوق، همانند یک دستورالعمل اجرائی بوده و عملیات لازم در زمان ارسال و یا دریافت داده را برای یک کامپیوتر مشخص می نماید. به منظور آشنائی و آنالیز فرآیند مبادله داده بین دو کامپیوتر موجود در یک شبکه به بررسی یک نمونه مثال کاربردی خواهیم پرداخت

زمانی که یک اتومبیل در کارخانه ای تولید می گردد، یک نفر تمامی کارها را انجام نخواهد داد. تولید یک اتومبیل بر اساس یک خط تولید انجام شده و همزمان با حرکت اتومبیل در خط تولید هر شخص بخش های متفاوتی را به آن اضافه نموده و زمانی که به انتهای خط تولید می رسیم، اتومبیل مورد نظر تولید و آماده استفاده خواهد بود.

وضعیت فوق در رابطه با داده ارسالی از یک کامپیوتر به کامپیوتر دیگر نیز صدق می کند. مدل OSI، قوانین لازم به منظور مبادله اطلاعات بین کامپیوتر ها را فراهم می نماید و داده ها در حین حرکت در هر لایه با توجه به مجموعه رهنمود هایی که OSI مشخص کرده است، تغییر شکل پیدا کرده و در نهایت از حالتی که در کامپیوتر قابل استفاده است به حالتی که از طریق کابل شبکه قابل ارسال باشد تبدیل می گردند و به این ترتیب داده ها از کامپیوتر مبدا قادر به ارسال به سایر کامپیوتر ها خواهد بود.

۸-۲- ساختار لایه ها در مدل مرجع OSI

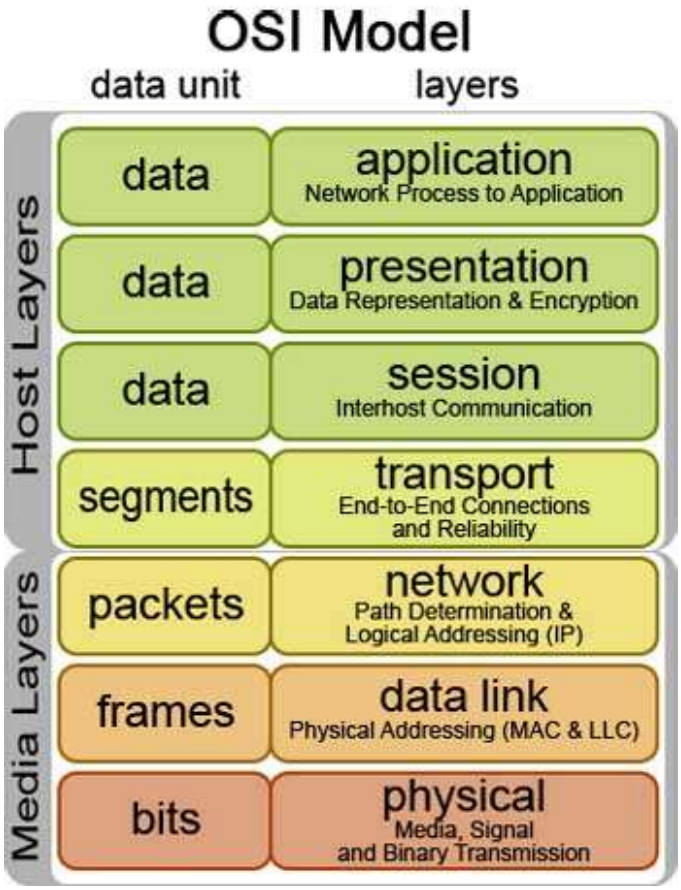
همانطور که گفته شد، کمیته IEEE به منظور جلوگیری از عدم هماهنگی بین محصولات و در نتیجه ناتوانی در برقراری ارتباط بین شبکه ای مدل مرجع OSI را معرفی کرد. این استاندارد تمامی فعالیتهایی را که باعث می شد اطلاعات از طریق شبکه و از کامپیوتری به کامپیوتر دیگر منتقل شود را در یک ساختار ۷ لایه ای در بر می گرفت. هر کدام از این لایه ها

مسئولیت انجام عملیات خاصی را برعهده دارند و در حقیقت ارسال و دریافت اطلاعات از طریق این لایه ها در کامپیوتر های فرستنده و گیرنده انجام خواهد شد.

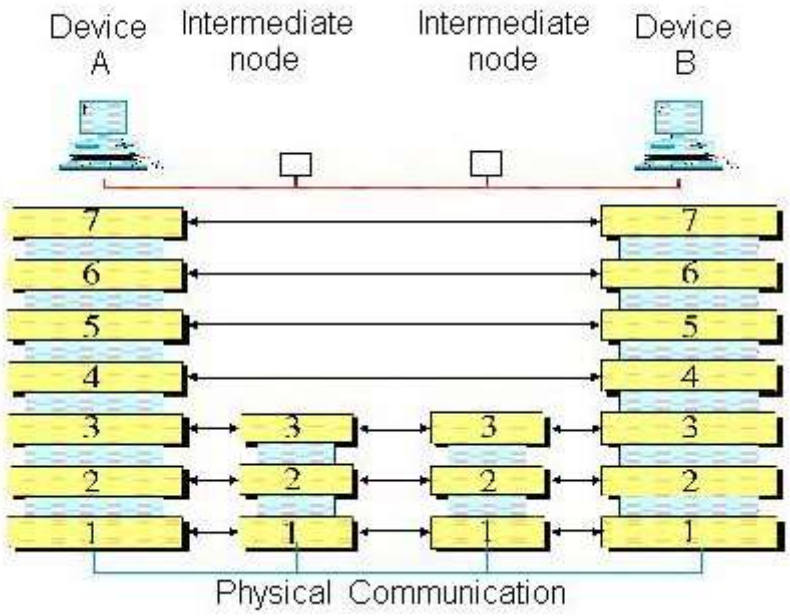
هنگام بررسی فرآیند انتقال اطلاعات بین دو کامپیوتر، مدل هفت لایه ای OSI روی هر یک از کامپیوتر ها پیاده سازی می گردد. در تحلیل این فرآیند ها می توان عملیات انتقال اطلاعات را بین لایه های متناظر مدل OSI واقع در کامپیوتر های مبدا و مقصد در نظر گرفت. این تجسم از انتقال اطلاعات را انتقال مجازی (Virtual) می نامند. اما انتقال واقعی اطلاعات بین لایه های مجاور مدل OSI واقع در یک کامپیوتر انجام می شود. در کامپیوتر مبدا اطلاعات از لایه فوقانی به طرف لایه تحتانی مدل OSI حرکت کرده و از آنجا به لایه زیرین مدل OSI واقع در کامپیوتر مقصد ارسال می شوند. در کامپیوتر مقصد اطلاعات از لایه های زیرین به طرف بالاترین لایه مدل OSI حرکت می کنند. عمل انتقال اطلاعات از یک لایه به لایه دیگر در مدل OSI از طریق واسطه ها یا Interface ها انجام می شود. این واسطه ها تعیین کننده سرویس هایی هستند که هر لایه مدل OSI می تواند برای لایه مجاور فراهم آورد.

مزیت این لایه ای بودن این است که پیچیدگی را کاهش می دهد بنابراین اگر سخت افزار یا نرم افزاری را تغییر دهیم دیگر تاثیری بر روی دیگر لایه ها نخواهد داشت.

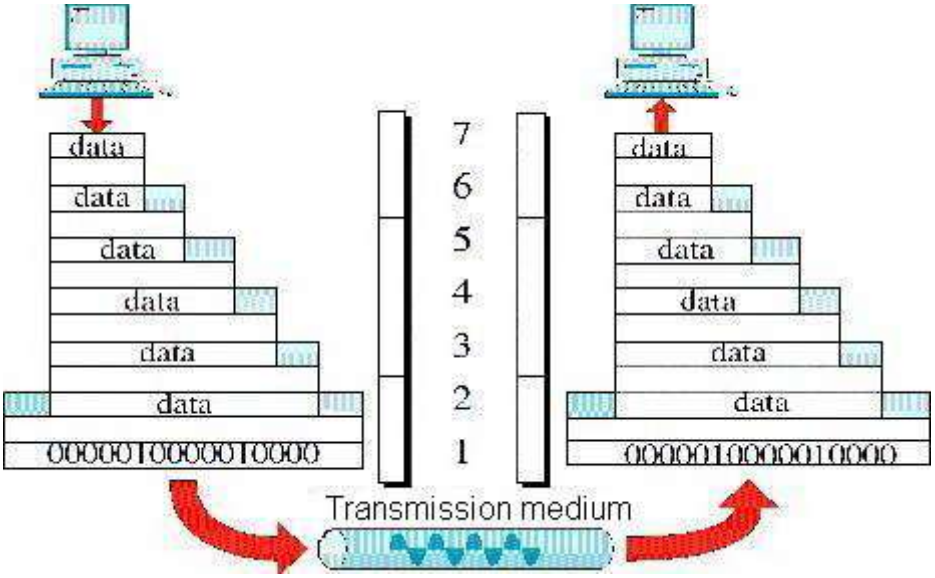
شکل زیر هفت لایه مدل OSI را نشان می دهد.



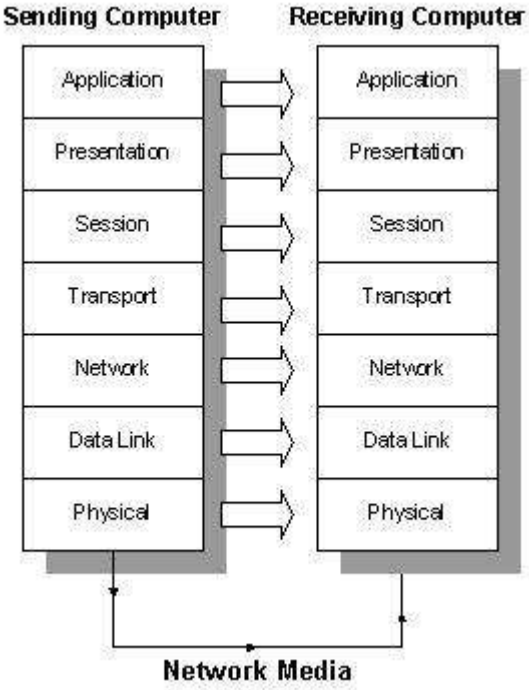
در شکل زیر لایه های متناظر ماشین A و ماشین B می توانند با هم ارتباط برقرار کنند، بنابراین هر لایه با لایه بالاتر یک پروتکل یکسان دارد. هیچ لایه ای نمی تواند مستقیماً اطلاعات را روی محیط ارتباطی قرار دهد، بلکه برای انتقال اطلاعات ابتدا لایه ۷ به لایه ۶ و لایه ۶ به لایه ۵ و به همین ترتیب انتقال می دهند تا اطلاعات روی محیط ارتباطی انتقال یابد.



هر لایه برای انجام دادن کار باید یک سری اطلاعات کنترلی داشته باشد تا گیرنده بتواند بر حسب آن اطلاعات کار انجام دهد. که هر لایه یک سری اطلاعات کنترلی به داده ها اضافه می کند و به لایه بعدی می فرستد.

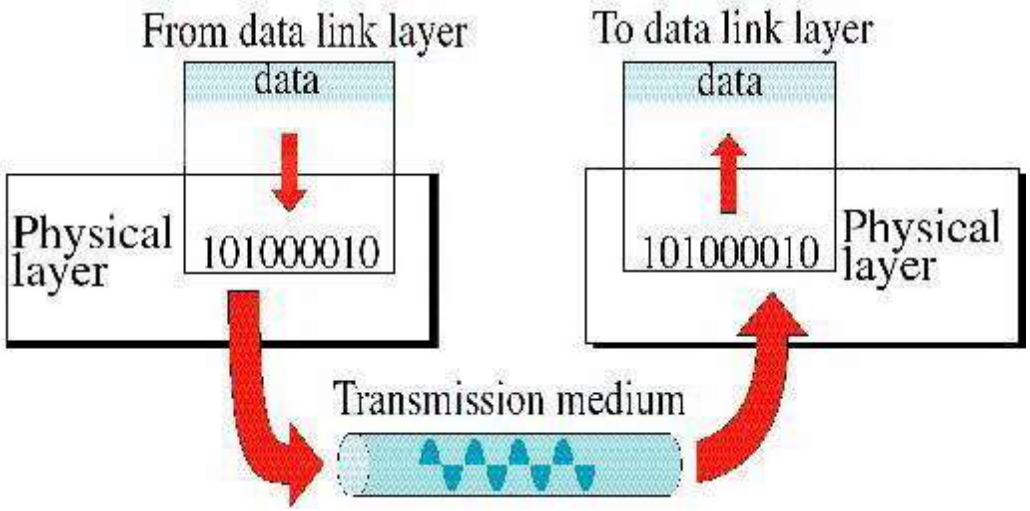


داده ها توسط یک برنامه و توسط کاربر تولید خواهند شد (نظیر یک پیام الکترونیکی). شروع ارسال داده ها از لایه Application است. در ادامه و با حرکت به سمت پایین، در هر لایه عملیات مربوطه انجام و داده هایی به بسته های اطلاعاتی اضافه خواهد شد. در آخرین لایه (لایه فیزیکی) با توجه به محیط انتقال استفاده شده، داده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



۸-۳- عملکرد هر یک از لایه های مدل مرجع OSI

۸-۳-۱- لایه Physical (لایه اول)

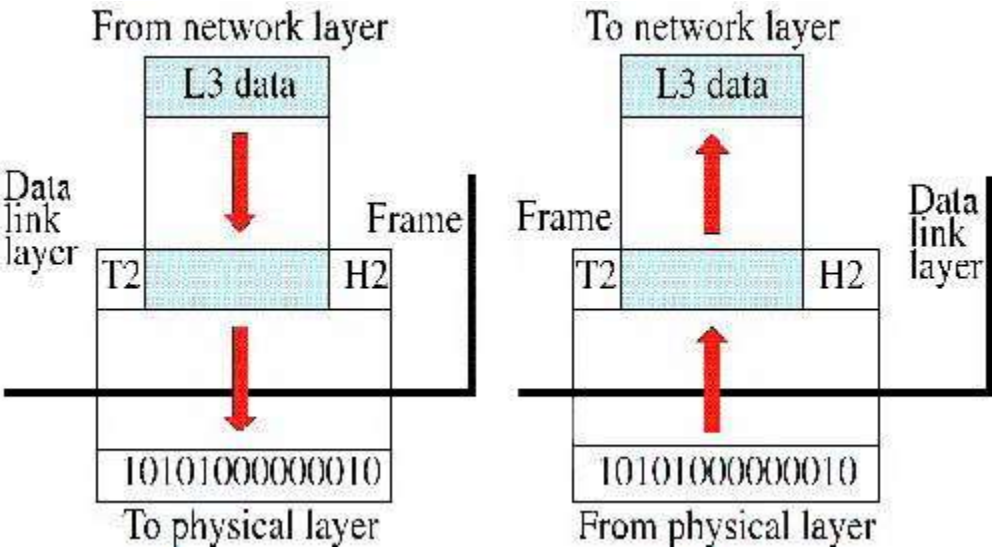


مسئولیت انتقال مجموعه ای از بیت ها از طریق رسانه ی فیزیکی بر عهده ی این لایه میباشد. در این لایه ابتدا توپولوژی فیزیکی، روش سیگنال دهی داخل رسانه انتقال و وسیله انتقال شبکه مورد بررسی قرار گرفته سپس اقدام به انتقال بیت ها می شود. از پروتکل هایی که در این لایه استفاده می شود، می توان از Ethernet ,ATM Gigabit و یا RS-233 نام برد.

خصوصیات به طور خلاصه

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

۸-۳-۲- لایه Datalink (لایه دوم)



این لایه تهیه کننده آدرس های سخت افزاری (MAC) و مشخص کننده خطاها و کنترل کننده جریان می باشد. این لایه وظیفه دارد تا اطلاعات دریافت شده از لایه شبکه را به قالبی منطقی به نام فریم (Frame) تبدیل کند. در کامپیوتر مقصد این لایه همچنین مسئول دریافت بدون خطای این فریم ها است. ما در لایه پیوند داده ها با توپولوژی منطقی شبکه سروکار داریم. از جمله توپولوژی BUS و توپولوژی RING.

در توپولوژی BUS ما اطلاعات را طوری فریم بندی می کنیم که هر کس در شبکه وجود دارد بتواند اطلاعات را دریافت کند حالا اگر آدرس فیزیکی موجود در فریم مربوط به خود او باشد اطلاعات را قبول کند، و گرنه به اطلاعات کار نداشته باشد که این نوع توپولوژی در شبکه های BUS وStar رواج دارد.

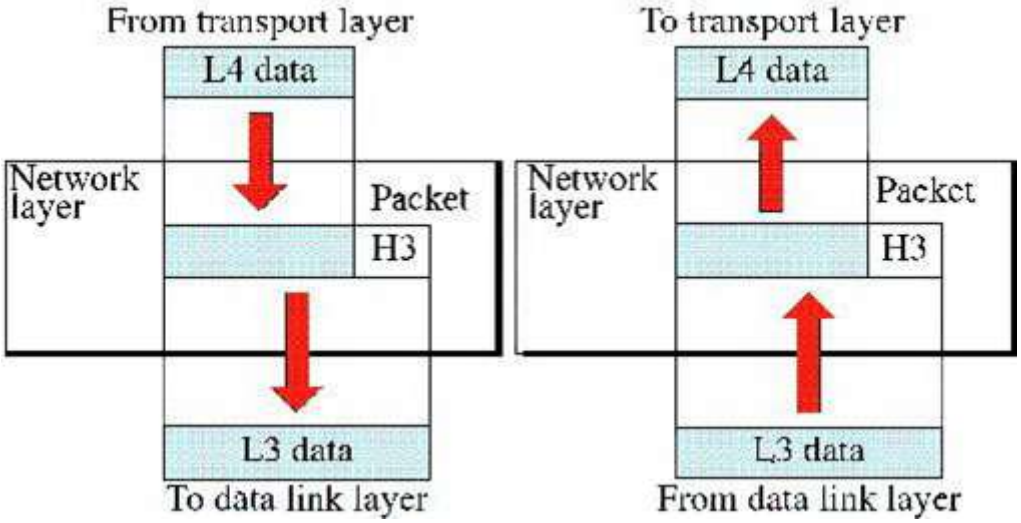
برای انتقال از یک دستگاه به دستگاه مشخص دیگر از توپولوژی منطقی RING استفاده می شود در اینجا هم توپولوژی فیزیکی شبکه میتواند RING یا STAR باشد.

آدرس سخت افزاری یا همان MAC Address، آدرس منحصر به فردی است که برای هر دستگاه وجود دارد.

خصوصیات به طور خلاصه

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

۸-۳-۳- لایه Network (لایه سوم)



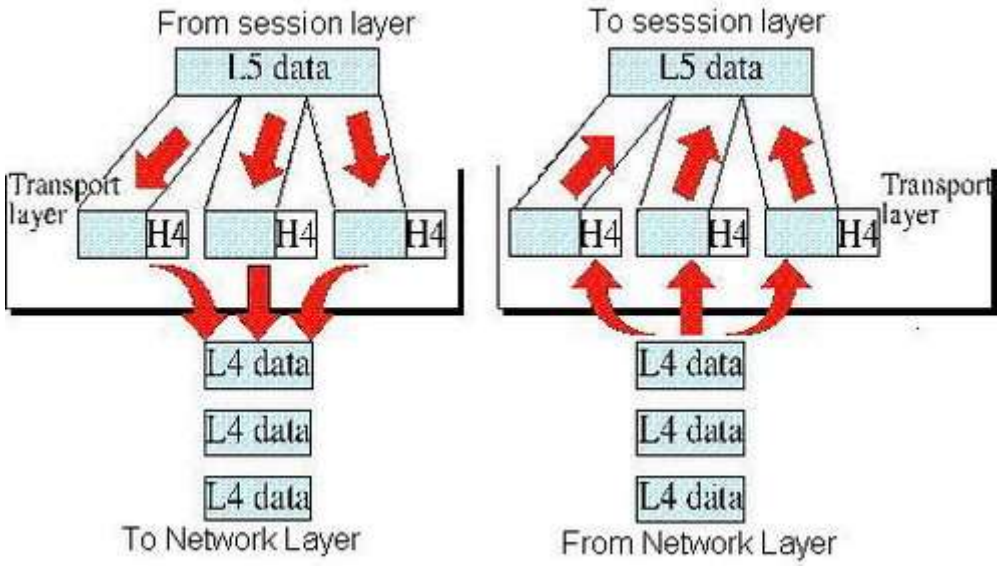
در این لایه با توجه به آدرس منطقی که به دستگاه ها در شبکه داده می شود مسیر یابی صورت میگیرد، در نتیجه ترافیک شبکه مدیریت می شود. میتوان کارهایی که در این لایه انجام می شود را به صورت زیر دسته بندی کرد:

۱. تهیه آدرس منطقی منحصر به فرد که برای هر بخش از شبکه در نظر گرفته می شود و با آدرس MAC متفاوت است.
۲. مسیر یابی داده و پیداکردن بهترین مسیر از بین چند مسیر.
۳. کنترل خطا، کنترل ارتباط و ترتیب بندی بسته ها.

خصوصیات به طور خلاصه

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

۸-۳-۴- لایه Transport (لایه چهارم)



مسئول ارسال و دریافت اطلاعات و کمک به رفع خطاهای ایجاد شده در طول ارتباط است. هنگامی که حین یک ارتباط خطایی بروز دهد، این لایه مسئول تکرار عملیات ارسال داده است.

دو نوع انتقال در لایه انتقال برقرار است:

۱- بدون اتصال (Connection Less):

در این انتقال ما به رسیدن پیام به مقصد کاری نداریم و منتظر رسیدن پیغام تصدیق نمی مانیم که این باعث کاهش قابلیت اطمینان و افزایش سرعت می شود.

۲- اتصال گرا (Connection Oriented):

در این انتقال در پی هر ارسال، منتظر رسیدن پیغام تصدیق می شویم که این باعث افزایش قابلیت اطمینان ولی کاهش سرعت می شود. در لایه انتقال مدیریتی بر روی کنترل جریان صورت میگیرد و در گیرنده امکان تصحیح خطا و مرتب کردن بسته ها وجود دارد.

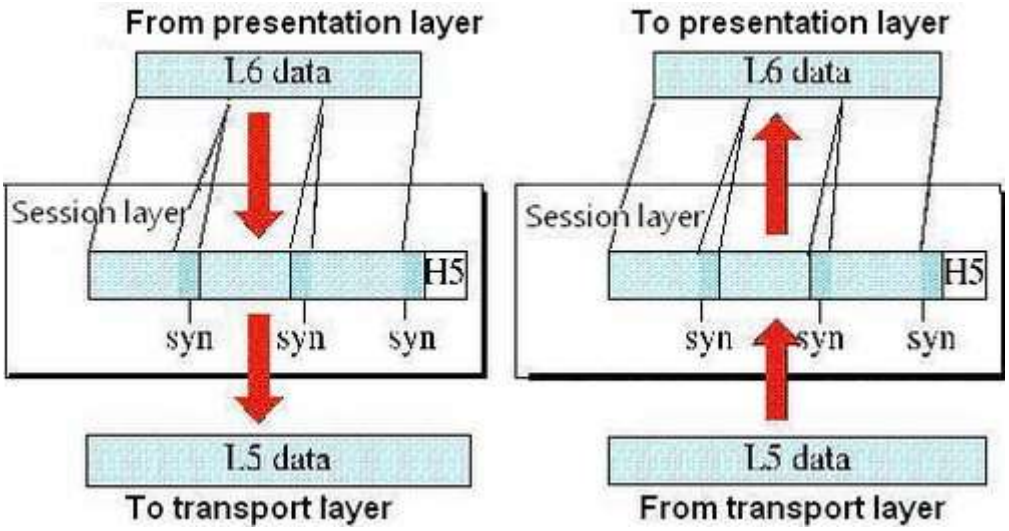
از پروتکلهای رایج در این لایه میتوان از TCP و یا UDP نام برد.

خصوصیات به طور خلاصه

- در ارتباط با رویکردهای متفاوت حمل داده بین کامپیوتر های میزبان
- حمل مطمئن داده

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

۸-۳-۵- لایه Session (لایه پنجم)



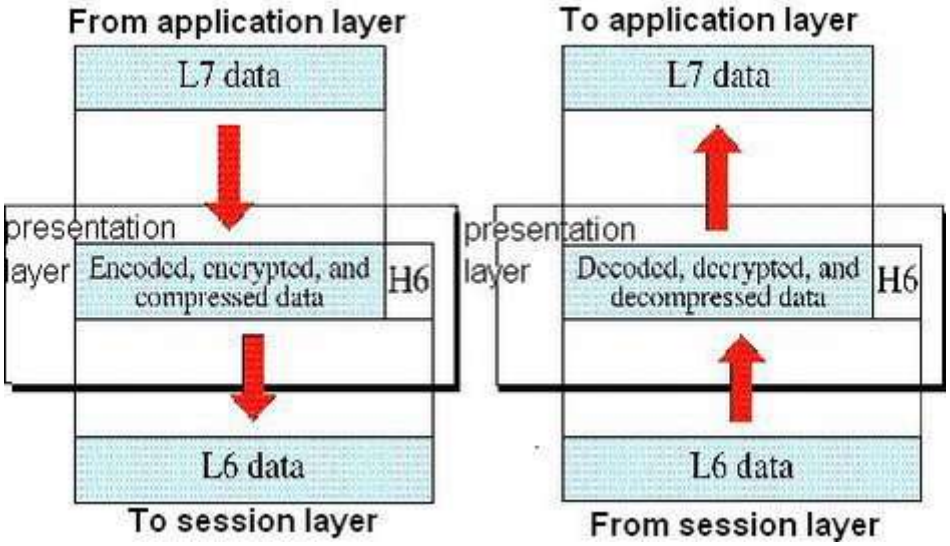
لایه ای است برای مدیریت ارتباط بین دو کاربر و در واقع ارائه کننده جلسه بین دو کاربر میباشد.

لایه جلسه یکسری قرارداد هایی را به اجرا می گذارد. مانند بررسی Username و Password کاربر در طول استفاده. در واقع این لایه بر برقراری اتصال بین دو برنامه کاربردی روی دو کامپیوتر مختلف واقع در شبکه نظارت دارد. همچنین تامین کننده همزمانی فعالیت های کاربر نیز هست.

خصوصیات به طور خلاصه

- ایجاد، مدیریت و خاتمه ارتباط برقرار شده بین برنامه ها

۸-۳-۶- لایه Presentation (ارائه) (لایه ششم)



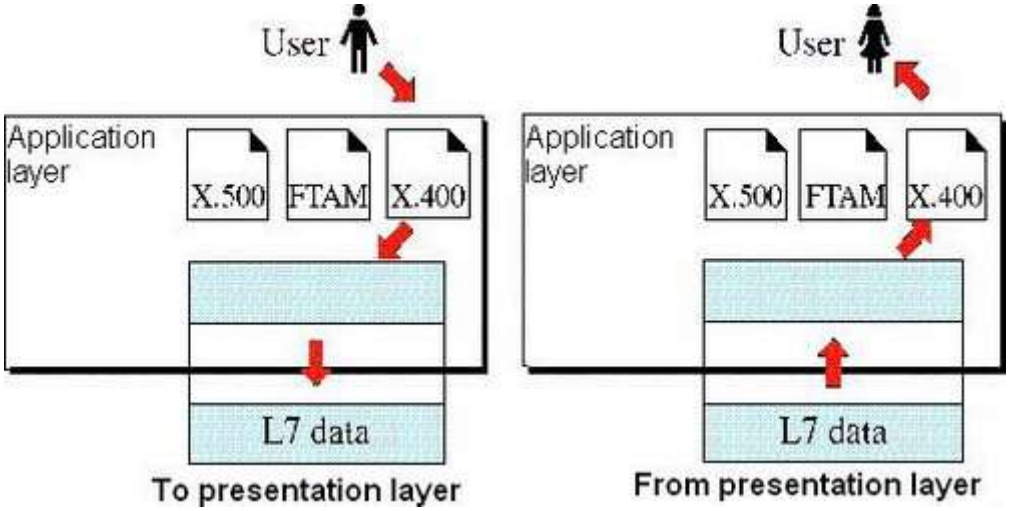
لایه ی Presentation راه هایی را فراهم میکند تا داده برای کاربر ارائه شود. پروتکل مربوط به این لایه فرمت داده را فراهم میکند و وقتی که می خواهیم داده را به لایه پایین تر بدهیم، لایه ی ارائه این داده را به گونه های Bit order Byte order, , Character order , File syntax به جمله انتقالیTransfer Syntax ترجمه میکند. در واقع این لایه تعیین کننده فرمت یا

قالب انتقال داده ها بین کامپیوتر های واقع در شبکه است. این لایه در کامپیوتر مبدا داده هایی که باید انتقال داده شوند را به یک قالب میانی تبدیل می کند. این لایه در کامپیوتر مقصد اطلاعات را از قالب میانی به قالب اولیه تبدیل می کند.

خصوصیات به طور خلاصه

- ایجاد اطمینان لازم در رابطه با قابل استفاده بودن داده برای سیستم دریافت کننده
- فرمت داده
- ساختمان های داده
- توافق در رابطه با گرامر انتقال داده برای لایه Application
- رمزنگاری داده

۸-۳-۷- لایه Application (لایه هفتم)



این آخرین لایه در اصل لایه ای است که کاربر تمام موارد قابل مشاهده را در آن مشاهده می کند. در این لایه دستگاه های فرستنده و گیرنده تعریف می شوند، کیفیت سرویس دهی و امنیت مشخص می شود. این لایه تامین کننده سرویس های پشتیبانی برنامه های کاربردی نظیر انتقال فایل، دسترسی به بانک اطلاعاتی و پست الکترونیکی است.

به عنوان مثال می توان به کارهای زیر اشاره کرد:

۱. انتقال فایل
۲. پیغام Email، وب و چت
۳. چاپ تحت شبکه
۴. بقیه عملیات هایی که دستگاه را با بقیه فرمانهای شبکه مرتبط میکنند.

نکته: معروفترین پروتکل این لایه FTP میباشد.

خصوصیات به طور خلاصه

- ارائه سرویس های شبکه به برنامه ها (نظیر پست الکترونیکی، ارسال فایل ها و...)
- تشخیص زمان لازم به منظور دستیابی به شبکه

۸-۴- نگاهی انتقادی به مدل OSI و پروتکل های آن

مدل OSI و پروتکل هایش هیچکدام کامل نیستند، و جا دارد برخی از نقاط ضعف آنها را بر شماریم. در این قسمت، برخی از نقاط ضعف مدل OSI را بررسی خواهیم کرد. در سال ۱۹۸۹، بسیاری متخصصان برجسته شبکه بر این باور بودند که آینده در بست متعلق به مدل OSI و پروتکل های آن است، و هیچ چیز نمی تواند در مقابل پیشرفت آن مقاومت کند. اما این اتفاق نیفتاد. چرا؟ نگاهی به گذشته درس های بسیاری را برای چشمان عبرت بین دارد، که می توان آنها را چنین خلاصه کرد:

۱. زمان نا مناسب
۲. تکنولوژی نامناسب
۳. پیاده سازی نامناسب
۴. سیاست های نامناسب

۸-۴-۱- زمان نامناسب

اولین عامل شکست مدل OSI زمان نامناسب بود. زمانی که یک استاندارد وضع می شود، زمان ارائه، اهمیت حیاتی در موفقیت و عدم موفقیت آن دارد. دیوید کلارک از دانشگاه MIT (برترین دانشگاه صنعتی جهان) فرضیه ای در زمینه استانداردها دارد که به **ملاقات فیل ها** معروف است. این فرضیه میزان فعالیت ها حول یک موضوع جدید را نشان می دهد. وقتی موضوعی برای اولین بار کشف می شود، گرداگرد آن سیلی از فعالیت های تحقیقی (به شکل بحث، مقاله و سخنرانی) فرا می گیرد. بعد از مدتی این فروکش می کند و بعد از اینکه صنعت به این موضوع علاقمند شد، موج سرمایه گذاری ها، به صورت پی در پی می آید.

بسیار مهم است که در محل تلاقی این دو فیل (موج تحقیق و موج سرمایه گذری) استانداردها به طور کامل وضع شوند. اگر استاندارد زودتر از موعد (قبل از پایان تحقیقات) نوشته شود، خطر آن است که موضوع به درستی درک نشده باشد و استاندارد ضعیف از آب در آید. اگر استاندارد دیرتر از موعد (بعد از شروع موج سرمایه گذاری) نوشته شود، شرکتهای بسیاری قبلاً (از مسیرهای مختلف) در آن سرمایه گذاری کرده اند، و این خطر وجود دارد که استانداردهای آنها را نادیده بگیرد. اگر فاصله این دو فیل خیلی کم باشد (همه عجله داشته باشند که کار را زودتر شروع کنند)، خطر آن است که نویسندگان استاندارد بین آن ها له شوند.

اکنون معلوم شده است که پروتکل های استاندارد OSI بین فیل ها له شده اند. وقتی که پروتکل های OSI پا به عرصه وجود گذاشتند، پروتکل های رقیب (TCP/IP) مدت ها بود که در مراکز تحقیقاتی و دانشگاه ها پذیرفته شده بودند. با اینکه هنوز موج سرمایه گذاری صنعتی در TCP/IP شروع نشده بود. اما بازار آکادمیک آنقدر بزرگ بود که شرکتهای بسیاری را تشویق به تولید محصولات TCP/IP کند. و وقتی OSI بالاخره از راه رسید، کسی نبود که داوطلبانه از آن پشتیبانی کند. همه منتظر بودند دیگری قدم اول را بر دارد.، قدمی که هرگز برداشته نشد و OSI در نطفه خفه شد.

۸-۴-۲- تکنولوژی نامناسب

دلیل دیگری که OSI هرگز پا نگرفت، آن بود که این مدل و پروتکل های آن هر دو ناقص و معیوب بودند. انتخاب هفت لایه برای این مدل بیشتر یک انتخاب سیاسی بود تا فنی، و در حالی که دو لایه آن (نشست و نمایش) تقریباً خالی بودند، در لایه های دیگر (لینک داده و شبکه) جای نفس کشیدن نبود.

مدل OSI (و سرویس ها و پروتکل های آن) به طور باور نکردی پیچیده است. اگر کاغذهای چاپی این استاندارد را روی هم بچینید. ارتفاع آن از نیم متر هم بیشتر خواهد شد. پیاده سازی پروتکل های OSI بسیار دشوار، و عملکرد آنها ناقص است. در این رابطه، نقل جمله جالبی از پاول موکاپتریس (Rose ،۱۹۹۳) خالی از لطف نیست:

سوال: از ترکیب یک گانگستر با یک استاندارد بین المللی چه چیزی بدست می آید؟

جواب: کسی پیشنهادی به شما می کند که از آن سر در نمی آورید.

مشکل دیگر مدل OSI، علاوه بر غیر قابل فهم بودن آن، این است که برخی از عملکرد های آن (مانند آدرس دهی، کنترل جریان داده ها و کنترل خطا)در تمام لایه ها تکرار می شود. برای مثال، سالتزر و همکارانش (۱۹۸۴) نشان دادند که کنترل خطا باید در بالاترین لایه انجام شود تا بیشترین تاثیر را داشته باشد، بنابراین تکرار آن در لایه های پائین تر نه تنها غیر ضروری است، بلکه باعث افت کارایی هم خواهد شد

۸-۴-۳- پیاده سازی نامناسب

با توجه به پیچیدگی بیش از حد مدل OSI و پروتکل های آن، جای تعجب نبود که اولین پیاده سازی های آن حجیم، سنگین و کند است. آنهایی که با این مدل کار کرده بودند، به زودی پشیمان شدند، و طولی نکشید که کلمه OSI مترادف شد با "کیفیت بد". بعد ها محصولات بهتری به بازار آمد، اما آوازه منفی OSI فراموش نشد.

از طرف دیگر، اولین پیاده سازی TCP/IP (که بخشی از سیستم عامل یونیکس دانشگاه برکلی بود) بسیار خوب از کار در آمد (و لازم به گفتن نیست که مجانی هم بود). افراد بسیاری با سرعت شروع به استفاده از آن کردند، طرفدار آن شدند، آن را توسعه دادند، و این باعث شد که باز هم به خیل طرفداران آن اضافه شود. در اینجا، بر خلاف OSI، مارپیچ رو به بالا می رفت، نه پایین.

۸-۴-۴- سیاست های نامناسب

دلیل استفاده از TCP/IP این بود که بسیاری از افراد (به ویژه در محیط های دانشگاهی) تصور می کردند که TCP/IP جزئی از یونیکس است، و یونیکس هم در آن دوران محبوبیتی فوق العاده داشت.

از سوی دیگر، این عقیده رواج داشت که OSI یک مخلوق دولتی (مخصوصا دولت های اروپایی و آمریکایی) است. البته این عقیده تا حدی درست بود، اما همین تصور هم که عده ای دیوان سالار دولتی بخواهد یک استاندارد دولتی را به زور به جا بیندازد، باعث شد تا برنامه نویسان و طراحان شبکه تمایلی از خود برای همکاری نشان ندهند. زبانهای برنامه نویسی PL/1 (که در دهه ۱۹۶۰ از سوی IBM به عنوان زبان آینده توسعه داده شد) و Ada (که وزارت دفاع آمریکا حامی آن بود) به همین دلیل دچار سرنوشتی مشابه شدند.

۸-۵- ساختار لایه ها در مدل TCP/IP

در قسمت قبل، معایب مدل OSI را مشاهده نمودید، در ادامه مدل دیگری به نام TCP/IP معرفی می کنیم. از آنجا که پروتکل TCP/IP در اینترنت بسیار مناسب است از این پروتکل در اغلب شبکه های داخلی نیز استفاده می شود این پروتکل برای کاربران حرفه ای شبکه بسیار کاربردی است. زیرا اتصال شبکه را تضمین میکند و به کاربر اجازه ارسال و دریافت فایل ها را به راحتی می دهد. حال به لایه های TCP/IP که برگرفته از مدل OSI است اشاره میکنیم.

۸-۵-۱- مفاهیم اولیه پروتکل TCP/IP

TCP/IP، یکی از مهمترین پروتکل های استفاده شده در شبکه های کامپیوتری است. اینترنت به عنوان بزرگترین شبکه موجود، از پروتکل فوق به منظور ارتباط دستگاه های متفاوت استفاده می نماید.

مقدمه

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

۸-۵-۲- معرفی پروتکل TCP/IP

از پروتکل TCP/IP، به منظور ارتباط در شبکه های بزرگ استفاده می گردد. برقراری ارتباط از طریق پروتکل های متعددی که در ۴ لایه مجزا سازماندهی شده اند، میسر می گردد. هر یک از پروتکل های موجود در پشته TCP/IP، دارای وظیفه ای خاص در این زمینه (برقراری ارتباط) می باشند. در زمان ایجاد یک ارتباط، ممکن است در یک لحظه تعداد زیادی از برنامه ها، با یکدیگر ارتباط برقرار نمایند. TCP/IP، دارای قابلیت تفکیک و تمایز یک برنامه موجود بر روی یک کامپیوتر با سایر برنامه ها بوده و پس از دریافت داده ها از یک برنامه، آنها را برای برنامه متناظر موجود بر روی کامپیوتر دیگر ارسال می نماید. نحوه ارسال داده توسط پروتکل TCP/IP از محلی به محل دیگر، با فرآیند ارسال یک نامه از شهری به شهر، قابل مقایسه است.

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

۸-۶- عملکرد هر یک از لایه های مدل TCP/IP

۸-۶-۱- لایه کاربردی

این لایه مجموع لایه های کاربردی، ارائه و جلسه در مدل OSI میباشد. این لایه داده اولیه را برای کاربر فراهم میکند و برای کاربران این دلیل خوبی است که به راحتی از آن استفاده کنند. در زیر به پروتکلهای این لایه اشاره میکنیم:

Telnet:

پروتکل کاربردی برای ارتباط از راه دور به کامپیوتر میزبان است که البته مدل ابتدایی است و مدلهای بالایی برای این کار وجود دارد از جمله RDP، ICA و یا Windows. البته Telnet ارتباط دقیق به پنجره جاری کامپیوتر میزبان است که از طریق پروتکل TCP/IP این عمل را انجام میدهد. البته از Telnet برای ارتباط با مسیریاب و همچنین تست اینکه ارتباط شبکه برقرار است یا نه استفاده می شود.

FTP:

پروتکلی است برای اتصال به کامپیوتر میزبان، فرستادن یا دریافت فایل بین کامپیوتر میزبان (راه دور) است که اتصال گرا بوده و انتقال داده را ضمانت میکند.

TFTP:

شبیه FTP است ولی برای مسافتهای طولانی استفاده شده و از پروتکل UDP استفاده میکند.

HTTP:

وقتی کاربران از اینترنت استفاده میکنند معمولاً دو کار عمده انجام می دهند: ارسال پیغام و یا تماشای صفحات وب. پروتکل HTTP امکان دریافت فایلهای HTML به همراه متن، عکس و.... را بوسیله مرورگر های وب فراهم میکند.

HTTPS:

HTTPS یا HTTP Over SSL همان پروتکل HTTP است با افزودن امنیت برای مرور صفحات با امنیت بالاتر

IMAP4/POP3:

دوپروتکل برای انتقال پیام الکترونیکی از طریق اینترنت هستند.

پروتکل POP3 برای دریافت پیغام در کلاینت و همچنین برای ارسال و دریافت در سرور استفاده می شود.

فرق بین POP3 و IMAP4 در اینست کهIMAP4 همانند یک فایل سرور از راه دور عمل میکند در حالی که POP3 در جایگاه اصلی کار میکند.

:SMTP

پروتکلی است برای ارسال پیغام الکترونیکی ولی قابلیت دریافت هم دارد و حجم آن کم است.

در واقع POP3 در حکم دریافت کننده پیغام و SMTP در حکم ارسال کننده پیغام کار میکند.

:NTP

پروتکلی است برای تنظیم زمان در اینترنت و مدیریت زمانی دریافت و ارسال اطلاعات در سرور.

:SNMP

پروتکلی است برای مشاهده و مدیریت وسایل شبکه که به مدیر شبکه در صورت بروز خطا، اخطار های لازم را میدهد.

۸-۶-۲- لایه انتقال

همانند لایه انتقال در پروتکل مدل OSI میباشد با پروتکلهای زیر:

:TCP

این پروتکل اتصال گرا، رسیدن داده ها به مقصد و درست به هم پیوستن بسته ها را تضمین مینماید.

کارکرد پروتکل TCP به نوع شبکه، توپولوژی و سرعت شبکه ربطی ندارد بلکه در این پروتکل با شماره گذاری هر بسته، بسته ها از مبدا به مقصد فرستاده می شود و در آنجا دوباره بسته ها به ترتیب شده و پیغام دریافت درست بسته ها، به مبدا ارسال می شود.

:UDP

اگر شبکه ای از TCP استفاده نکند از UDP استفاده میکند در پروتکل UDP که برای ارسال داده های کم و برای سرعت بالا استفاده می شود هیچگونه پیغام تصدیقی مبنی بر رسیدن درست داده به مقصد ارسال نمی شود.

۸-۶-۳- لایه شبکه

برگرفته از همان لایه شبکه در مدل OSI است با این تفاوت که فقط از پروتکل IP استفاده میکند. زیر پروتکلهای این لایه عبارتند از:

:ARP

پروتکلی برای مشخص کردن آدرس میباشد، یعنی آدرس فیزیکی و آدرس IP را با یکدیگر Map (نگاشت) می کند. این پروتکل در حقیقت برای زمانی که قرار است از یک کامپیوتر در یک ساختمان به کامپیوتر دیگر در ساختمان دیگر اطلاعاتی فرستاده شود و مابین یک مسیریاب بر اساس آدرس فیزیکی کار می کند، استفاده می شود. در اینجا از این پروتکل برای تبدیل آدرس IP به فیزیکی و بر عکس استفاده می شود.

:ICMP

پروتکلی است برای کنترل پیغام و گزارش خطا به این معنی که وقتی از دستور Ping برای اینکه ببینیم که میتوانیم با کامپیوتر میزبان ارتباط برقرار کنیم یا نه استفاده میکنیم، در حقیقت در حال استفاده از ICMP هستیم.

:IP

یک پروتکل بدون اتصال است و تمام کارها در مدل TCP/IP مبتنی بر این پروتکل IP میباشد این پروتکل آدرس وسیله میزبان و وسایل شبکه را برای بر قراری ارتباط فراهم میکند.

۸-۶-۴- لایه Network Interface (Physical)

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

۸-۷- نگاهی انتقادی به مدل TCP/IP

مدل TCP/IP و پروتکل های آن نیز مشکل خاص خود را دارند.

اول اینکه، در این مدل مفاهیم سرویس، واسط و پروتکل به روشنی از یکدیگر تفکیک نشده اند. کاری که در مدل OSI به خوبی انجام شده است. به همین دلیل نمی توان از TCP/IP به عنوان ابزاری برای طراحی و توسعه شبکه های جدید استفاده کرد.

دوم اینکه، مدل TCP/IP به هیچ عنوان یک مدل کلی نیست، و نمی توان از آن برای توصیف شبکه های غیر TCP/IP استفاده کرد. برای مثال، توصیف بلوتوث با مدل TCP/IP به کلی غیر ممکن است.

سوم این که، با در نظر گرفتن مفاهیم شبکه های چند لایه، لایه -میزبان- به شبکه اساسا یک لایه واقعی نیست، بلکه فقط یک واسط (بین لایه های شبکه و لینک داده) است. در واقع، این یکی از مهمترین جاهایی است که مدل TCP/IP مفاهیم واسط و لایه ها را با هم ترکیب کرده است.

چهارم اینکه، در مدل TCP/IP هیچ تمایزی بین لایه های فیزیکی و لینک داده نیست (و حتی حرفی از آن ها به میان نیامده است). اینها دو لایه کاملاً متفاوت هستند. لایه فیزیکی با مشخصات کابل و فیبر نوری و کانال های مخابراتی سر و کار دارد، در حالی که وظیفه لایه پیوند داده شکستن لایه ها به قطعات کوچکتر و اطمینان از تحویل صحیح آنها به مقصد است. در یک مدل کامل این دو لایه باید از هم جدا باشند؛ کاری که در مدل TCP/IP انجام نشده است.

در تصویر زیر تشابه لایه ها در دو مدل مرجع OSI و TCP/IP را مشاهده میکنید:

<table>
<tr><td>Application</td><td rowspan="3">Application</td></tr>
<tr><td>Presentation</td></tr>
<tr><td>Session</td></tr>
<tr><td>Transport</td><td>Transport</td></tr>
<tr><td>Network</td><td>Internet</td></tr>
<tr><td>Data Link</td><td rowspan="2">Network Address</td></tr>
<tr><td>Physical</td></tr>
</table>

فصل ۹

ساخت شبکه های مجازی با نرم افزار Virtual Box

۹-۱- مقدمه

بسیاری از مباحث عملی مطرح شده در این جزوه، جهت انجام نیاز به دو یا چند کامپیوتر دارند به طوری که این کامپیوتر ها با یکدیگر شبکه شده باشند. اما از آنجایی که برای افراد سخت است که در خانه خود یک شبکه کامپیوتری راه اندازی کنند (به خاطر محدودیت های سخت افزاری)، لذا تصمیم گرفتیم که در ابتدای آموزش های عملی، آموزش شبیه سازی اجرای همزمان چندین سیستم عامل روی یک سیستم عامل به گونه ای که این سیستم عامل ها بتوانند با یکدیگر شبکه شوند را آموزش دهیم. مزیت این کار این می باشد که افراد می توانند چندین سیستم را به صورت نرم افزاری با یکدیگر شبکه نموده و مباحث عملی مطرح شده را به راحتی کار نمایند. مزیت دیگر نیز این است که در کلاس های آموزش عالی، معمولاً جهت جلوگیری از خرابی نرم افزاری کامپیوتر ها، آن ها را Freeze می کنند؛ تا تغییرات نرم افزاری را بی اثر سازند؛ اما با شبیه سازی می توان ابتدا نرم افزار شبیه ساز را نصب نمود و سپس به تعداد دلخواه روی آن سیستم عامل نصب کرد. نرم افزاری که ما در این فصل آموزش می دهیم، نرم افزار Oracle VM VirtualBox می باشد.

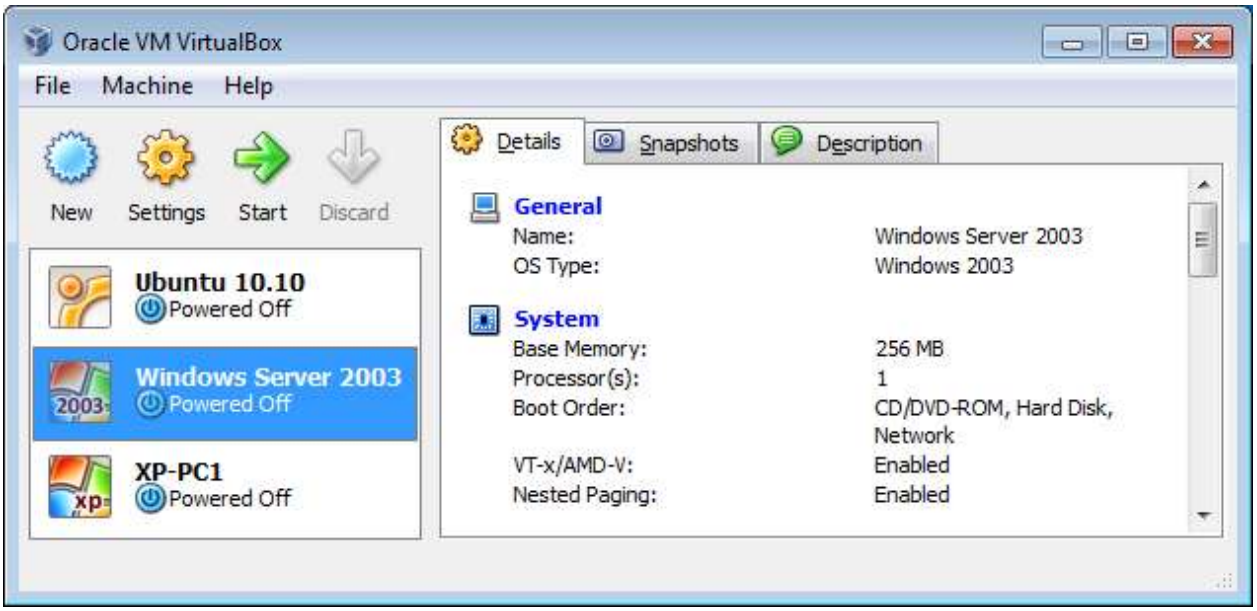
۹-۲- Oracle VM VirtualBox

جهت شبیه سازی اجرای همزمان چندین سیستم عامل، نرم افزار های متعددی وجود دارند، نرم افزار هایی از قبیل: VMware Work Station، Microsoft Virtual PC، Oracle VM Virtual Box و ... . اما دلیل اینکه ما نرم افزار Oracle VM VirtualBox را انتخاب نمودیم این است:

۱. نرم افزار پر قدرتی است.
۲. رایگان می باشد.
۳. کم حجم است (۷۵ مگابایت).

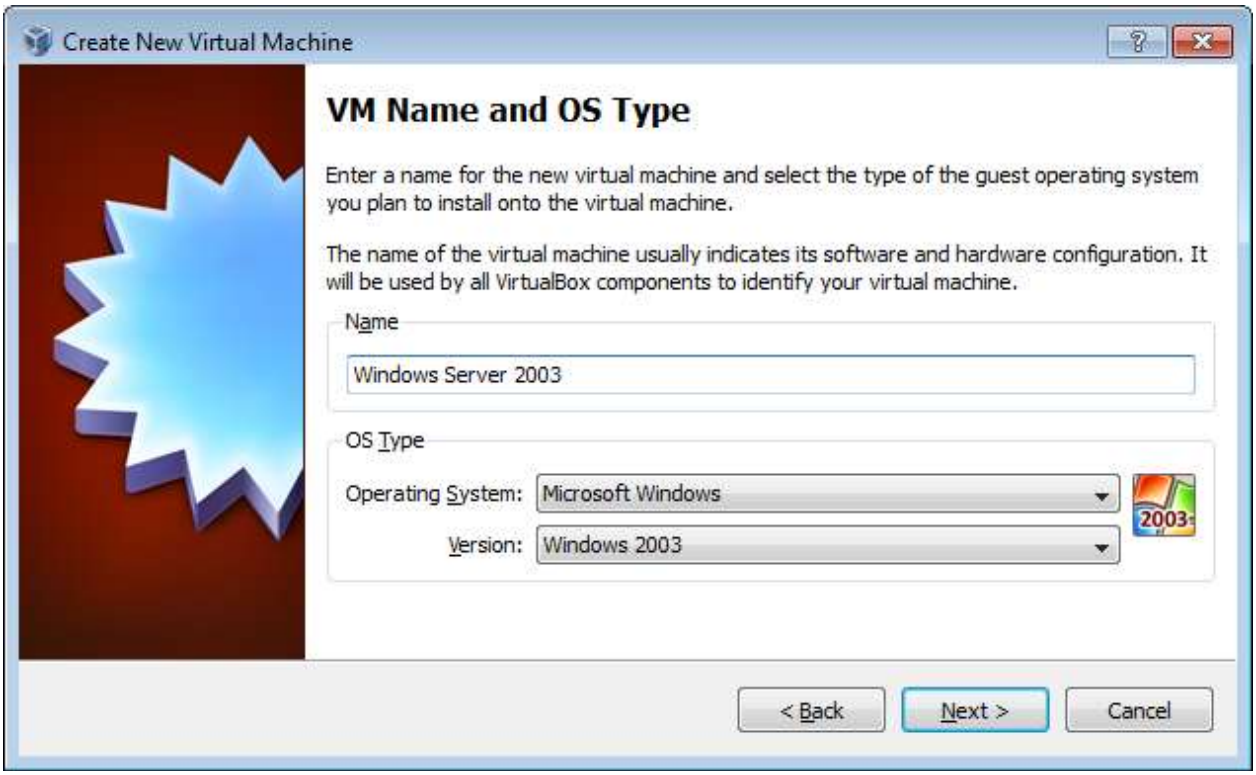
۴. بسیار سبک و راحت اجرا می شود.

در ادامه این نرم افزار را به اختصار Virtual Box می نامیم. VM در Oracle VM VirtualBox مخفف Virtual Machine و به معنای ماشین مجازی می باشد. در گام اول، این نرم افزار را دانلود نموده و آن را نصب نمایید. پس از نصب نرم افزار و باز کردن آن، صفحه ای مانند صفحه زیر مشاهده می نمایید:

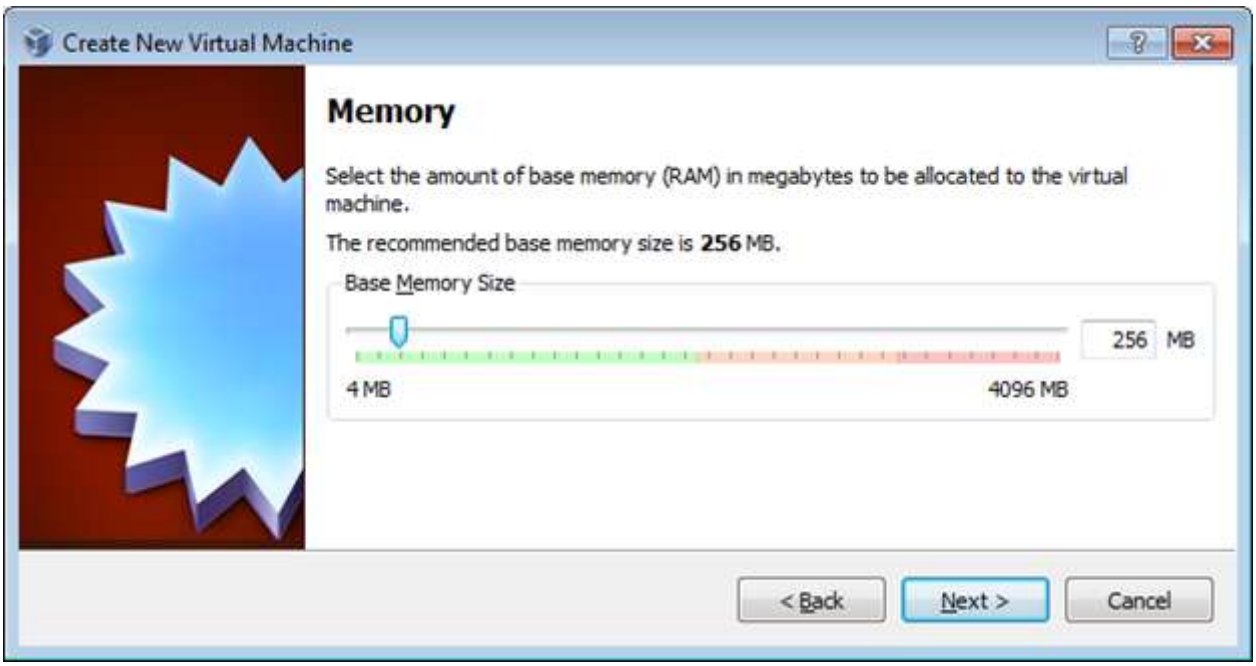


در سمت چپ، لیست سیستم عامل های نصب شده را مشاهده می نمایید و در سمت راست نیز با انتخاب هر سیستم عامل، قادر به مشاهده جزئیات آن خواهید بود. در بالا نیز دکمه هایی جهت ساخت سیستم عامل جدید (New)، انجام تنظیمات روی سیستم عامل های موجود (Settings) و راه اندازی یکی از سیستم عامل های موجود (Start) وجود دارد. با این نرم افزار امکان اجرای همزمان چندین سیستم عامل نیز وجود دارد.

ما بحث را با آموزش نصب یک سیستم عامل مجازی آغاز می کنیم. بدین منظور در صفحه اصلی روی دکمه New کلیک کنید. بدین ترتیب صفحه خوش آمد گویی باز می شود. روی Next کلیک کنید. در صفحه بعدی نوع سیستم عامل مورد نظر خود را انتخاب نموده و نامی دلخواه برای آن انتخاب نمایید. سعی نمایید که نام وارد شده پر مفهوم بوده و بیانگر خود سیستم عامل باشد. روی دکمه Next کلیک کنید.

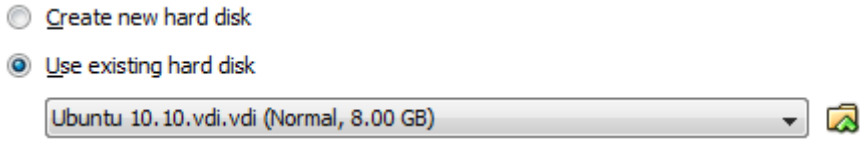


در صفحه بعد، میزان حافظه RAM که به این سیستم عامل تخصیص می دهید را بر حسب مگابایت وارد نمایید. توصیه می شود که همین مقدار پیش فرض را انتخاب نمایید. مقدار پیش فرض برای ویندوز سرور ۲۰۰۳، برابر با 256 MB می باشد.



در صفحه بعد، بایستی یک فایل را به عنوان هارد دیسک سیستم عامل مورد نظر انتخاب نمایید. سیستم عامل مجازی این فایل را به صورت یک هارد دیسک مجزا می بیند و هر مقدار که اندازه سیستم عامل مجازی شما رشد کند (مثلاً با نصب نرم افزار های مختلف)، اندازه این فایل نیز بزرگتر می شود.

اگر از قبل یک فایل به عنوان هارد دیسک دارید و اکنون می خواهید این فایل به عنوان هارد دیسک این سیستم عامل جدید استفاده شود (مثلاً قبلاً یک سیستم عامل مجازی نصب کرده اید و اکنون می خواهید این سیستم عامل را روی ۱۰ کامپیوتر استفاده نمایید، لذا فایل مربوط به هارد این سیستم عامل را روی هر ۱۰ کامپیوتر کپی می نمایید)، گزینه دوم یعنی Use Existing Hard Disk را انتخاب نموده و سپس روی علامت کلیک نمایید.

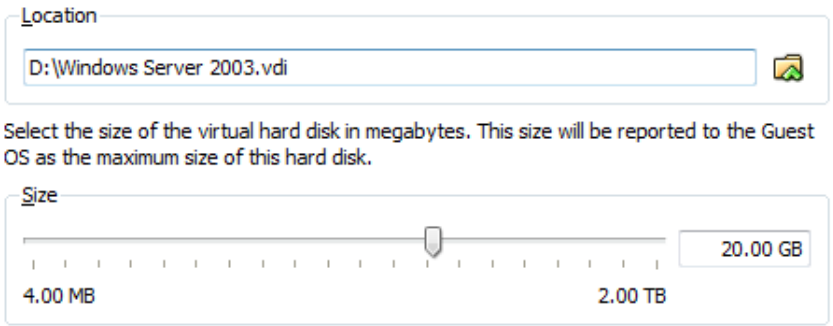


در صفحه باز شده، روی دکمه Add کلیک نموده و سپس فایل مورد نظر را انتخاب نمایید.

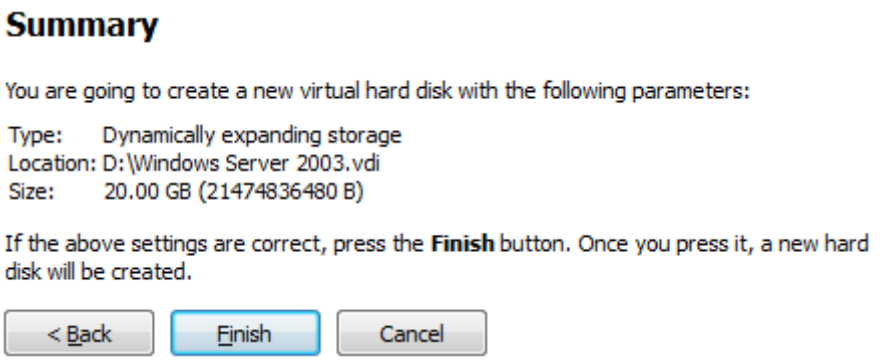
پس از انتخاب فایل مورد نظر، روی Select کلیک کنید. اما اگر هیچ فایلی به عنوان هارد دیسک ندارید و می خواهید فایلی جدید به عنوان هارد دیسک بسازید، گزینه Create New Hard Disk را انتخاب نموده و سپس روی Next کلیک نمایید.

صفحه ایجاد هارد جدید باز می شود. پس از عبور از صفحه خوش آمد گویی، وارد صفحه نوع هارد دیسک از لحاظ روش گسترش سایز می شوید. در این صفحه اگر گزینه Dynamically Expanding Storage را انتخاب نمایید، هارد دیسک شما، ابتدا اندازه صفر دارد (قبل از نصب سیستم عامل مجازی) و به موازات رشد سیستم عامل مجازی، اندازه فایل نیز بزرگتر می شود. اما اگر گزینه Fixed-Size Storage را انتخاب نمایید، بدین معنا است که اگر اندازه هارد را مثلاً 10 GB انتخاب نمودید، فایل شما نیز از همان ابتدا 10 GB فضا اشغال می کند، حتی اگر هیچ سیستم عاملی هم نصب نکرده باشید. توصیه می شود گزینه Dynamically Expanding Storage را انتخاب نمایید. در نهایت روی Next کلیک کنید.

در صفحه بعدی بایستی اندازه هارد دیسک مورد نظر و محل فایل متناظر با آن را تعیین نمایید. توصیه می شود که اندازه پیش فرض را قبول نموده و فایل متناظر با هارد دیسک را نیز در جایی ذخیره نمایید که به اندازه کافی فضای خالی داشته باشد. سپس روی دکمه Next کلیک کنید.

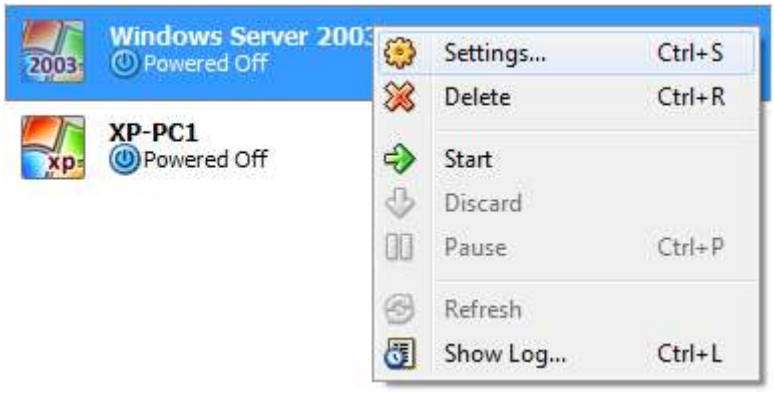


در پایان، نرم افزار، خلاصه ای از کارهای انجام شده را به شما نشان می دهد. جهت اتمام عملیات ساخت هارد و معرفی سیستم عامل جدید، روی دکمه Finish کلیک نمایید.

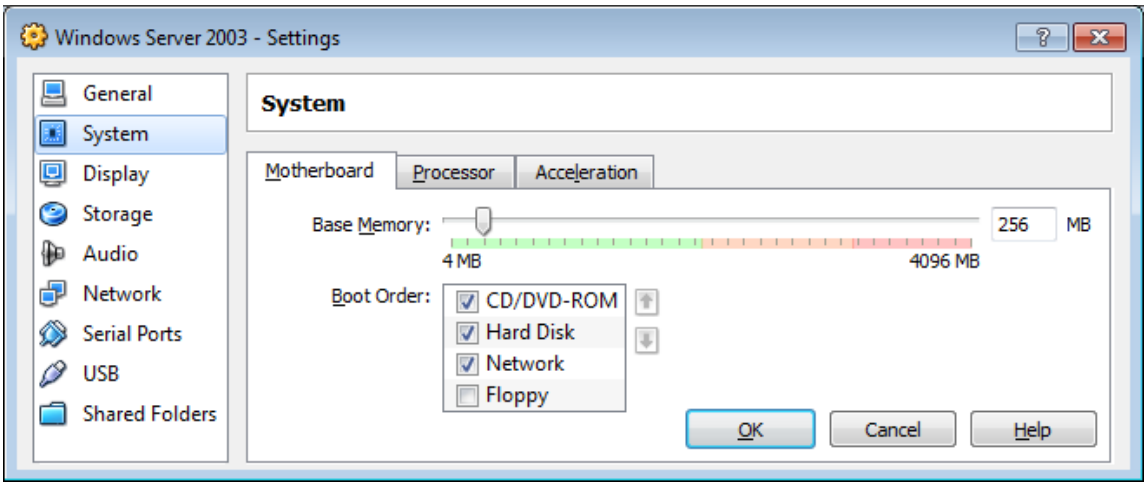


تا اینجا شما فقط سیستم عامل جدید خود را به همراه هارد دیسک آن و مقدار حافظه RAM به نرم افزار Virtual Box معرفی نموده اید. اما هنوز سیستم عامل خود را نصب نکرده اید.

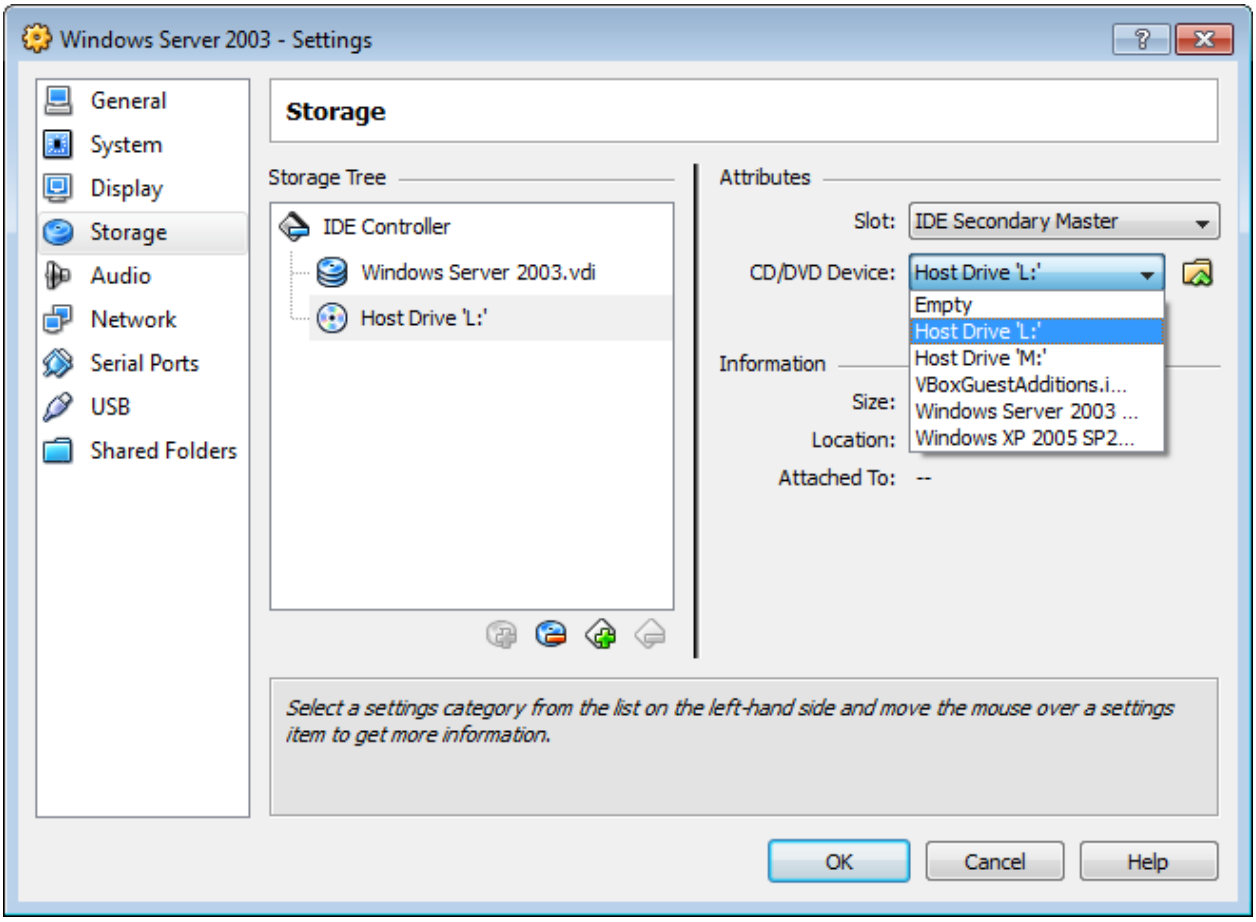
حال نوبت به عملیات نصب سیستم عامل جدید می رسد. عملیات نصب سیستم عامل مجازی، دقیقا مانند سیستم عامل های واقعی می باشد. بدین منظور بایستی ابتدا تنظیماتی را روی سیستم عامل مجازی خود انجام دهیم. لذا روی سیستم عامل مورد نظر راست کلیک نموده و گزینه Settings را انتخاب نمایید.



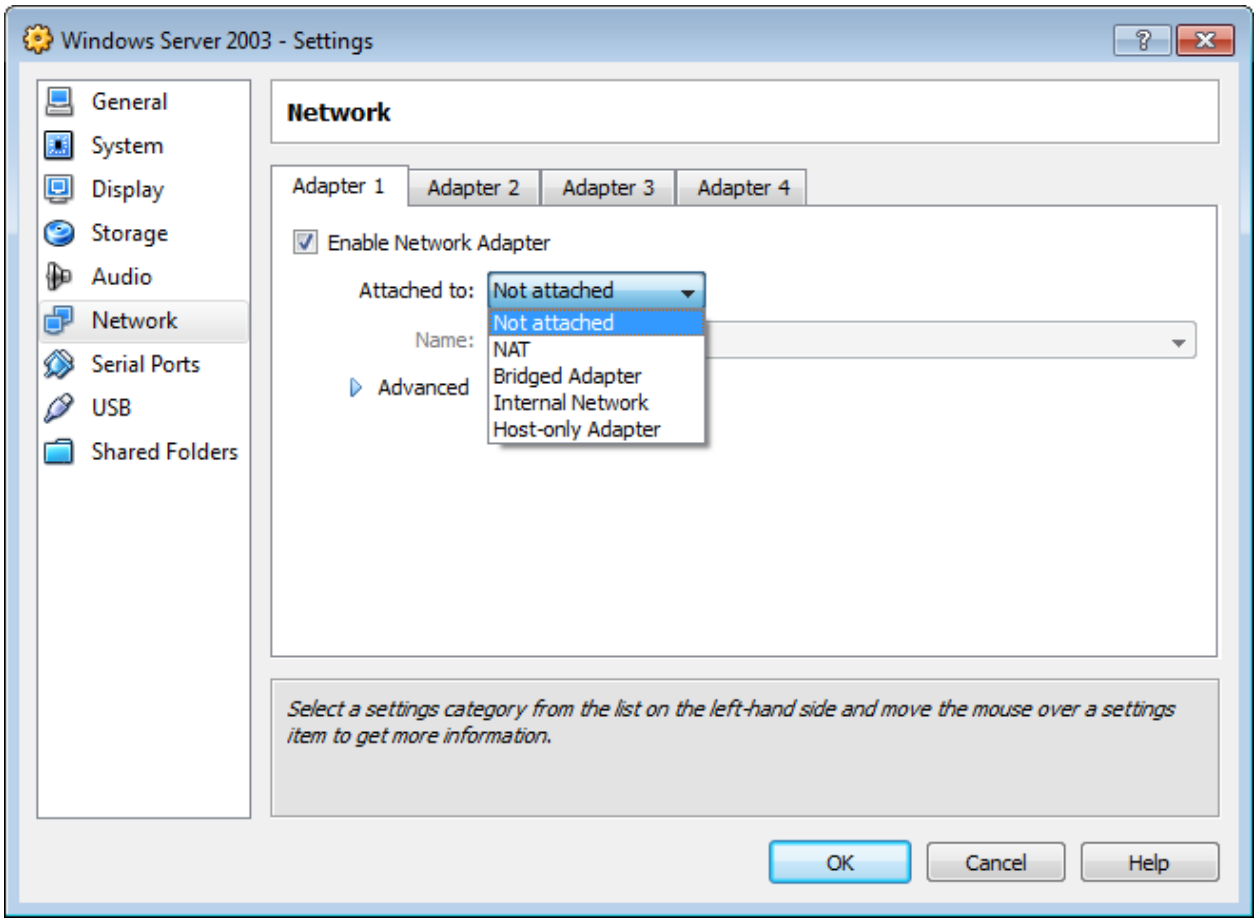
شما از طریق این قسمت می توانید تنظیماتی را روی سیستم مجازی خود انجام دهید. مثلاً از طریق قسمت System، می توانید میزان RAM مورد استفاده و نیز ترتیب دستگاه ها جهت بوت شدن (راه اندازی) سیستم عامل را تعیین نمایید. بهتر است مانند شکل زیر تعیین نمایید که بوت شدن ابتدا از هارد دیسک شروع شده و سپس به سراغ سی دی رام برود.



در مراحل قبل، مشخص نمودیم که سیستم عامل مجازی، از کدام فایل به عنوان هارد دیسک خود استفاده نماید. حال بایستی به سیستم عامل مجازی خود بگوییم که از کدام یکی از دیسک های نوری ما به عنوان سی دی رام خود استفاده نماید. در نرم افزار Virtual Box این امکان وجود دارد که بتوان یک فایل Image با پسوند iso. را به عنوان سی دی رام یک سیستم عامل مجازی انتخاب نمود. جهت انجام تنظیمات سی دی رام، ابتدا وارد قسمت Storage شوید. در سمت چپ، ابتدا Host Drive را انتخاب نموده و سپس در سمت راست، یکی از دیسک های نوری سیستم را به عنوان سی دی رام انتخاب نمایید. اینکه چگونه یک فایل Image را به عنوان سی دی رام انتخاب کنیم را جلوتر توضیح خواهیم داد. از آنجا که در اکنون اولویت اصلی ما نصب سیستم عامل می باشد، سی دی شامل سیستم عامل را درون درایو سی دی قرار داده و در قسمت Storage، این درایو سی دی را به عنوان سی دی رام سیستم عامل مجازی انتخاب می کنیم.

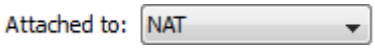


مهمترین قسمت تنظیمات سیستم عامل مجازی، تنظیمات شبکه آن می باشد. تنظیمات این بخش، تاثیر زیادی بر کار ما دارد؛ زیرا هدف ما از راه اندازی سیستم عامل مجازی، شبکه کردن چندین سیستم عامل به صورت مجازی می باشد. جهت انجام تنظیمات شبکه، وارد قسمت Network شوید. در Virtual Box، امکان تعریف ۴ کارت شبکه به صورت همزمان وجود دارد که ما در اینجا فقط با یک آداپتور کار داریم. چگونگی کارکرد شبکه را در ۵ وضعیت مختلف می توان تعیین نمود. در ادامه این ۵ حالت را توضیح می دهیم. فرض کنید که سیستم عامل اصلی ما، ویندوز ۷ می باشد که ما Virtual Box را روی آن نصب نموده ایم. روی Virtual Box نیز دو سیستم عامل Windows XP و Windows Server 2003 نصب نموده ایم که این دو سیستم عامل های مجازی ما می شوند.



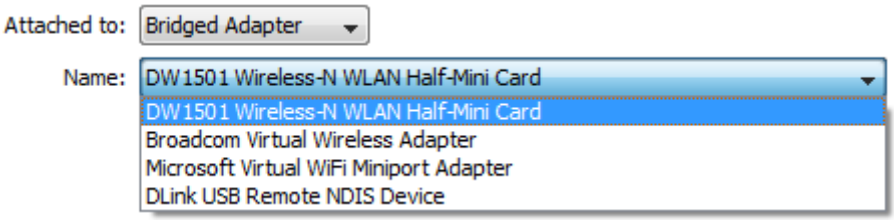
– **Not Attached:** این گزینه بدین معنا است که سیستم عامل مجازی ما، اصلا کارت شبکه ندارد.

– **NAT:** بدین معنی می باشد که سیستم عامل مجازی ما، با هیچ سیستم دیگری شبکه نیست، ولی امکان اتصال به اینترنت را دارد. یعنی دقیقا مانند یک سیستم عامل مستقل عمل می کند.



¶

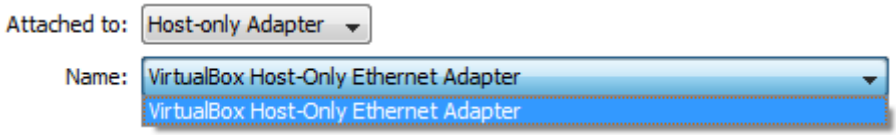
– **Bridge Adapter:** توسط این قسمت می توان تعیین نمود که سیستم عامل مجازی، بتواند توسط یکی از تجهیزات سیستم عامل اصلی (Windows 7) به اینترنت متصل شود. بعد از انتخاب این گزینه، بایستی تجهیزی که می خواهیم به کمک آن به اینترنت متصل شویم را نیز تعیین نماییم.



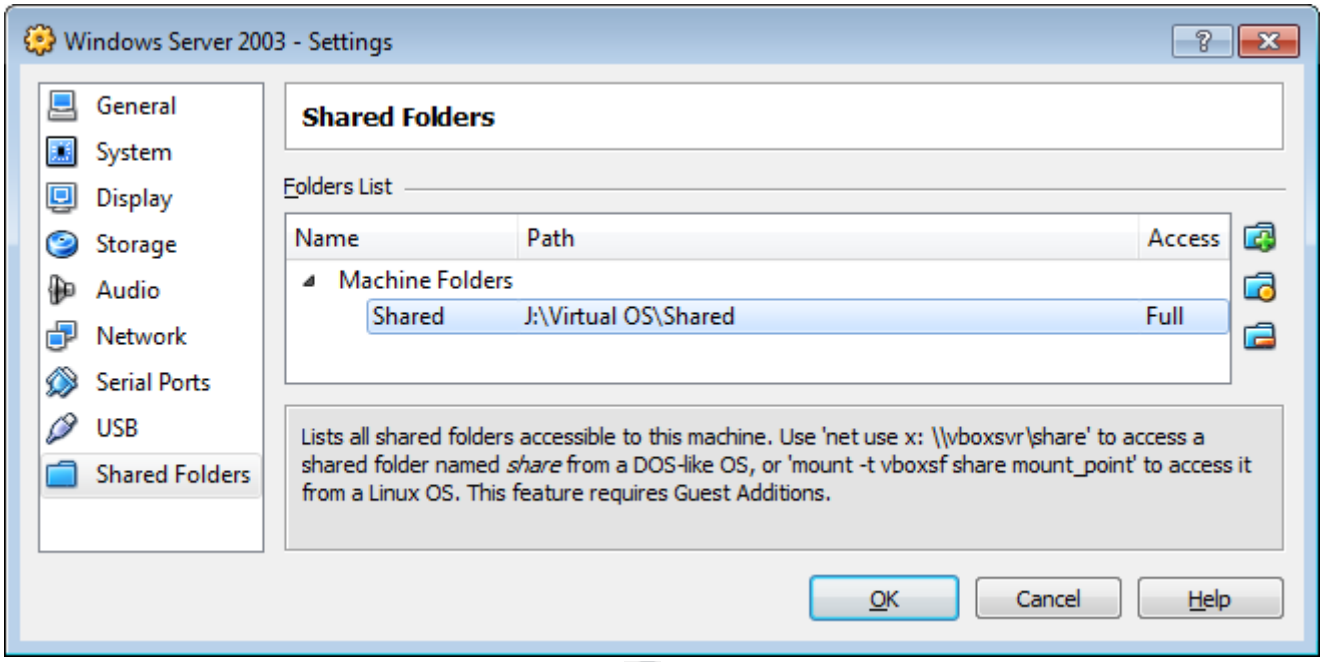
– **Internal Network:** از این گزینه برای شبکه کردن سیستم عامل های مجازی با یکدیگر استفاده می شود (در اینجا Windows XP و Windows Server 2003). اگر قصد داریم کار های عملی این فصل را با سیستم عامل های مجازی انجام دهیم، بایستی چندین سیستم عامل مجازی را با یکدیگر شبکه کنیم که برای شبکه کردن آن ها بایستی از گزینه Internal Network استفاده نماییم. بعد از انتخاب این گزینه، بایستی نامی برای شبکه مجازی خود انتخاب کنیم که طبعا سیستم عامل هایی با یکدیگر شبکه می شوند که هم مجازی بوده و هم نام شبکه اشان با یکدیگر برابر باشد.

– **Host-Only Adapter:** از این گزینه برای شبکه کردن سیستم عامل مجازی (در اینجا Windows XP یا Windows Server 2003) با سیستم عامل واقعی (در اینجا Windows 7) استفاده می شود. نرم افـزار Virtual Box هنگـام نصـب، یـک آداپتور شبکه به سیستم عامل واقعی به نام VirtualBox Host-Only Network ایجاد می کند. که اگر قصد داریـد بـا گزینـه Host-Only Adapter، سیستم عامل مجازی را با سیستم عامل واقعی شبکه کنید، بایسـتی ایـن کانکشـن را فعـال (Enable) سازید.

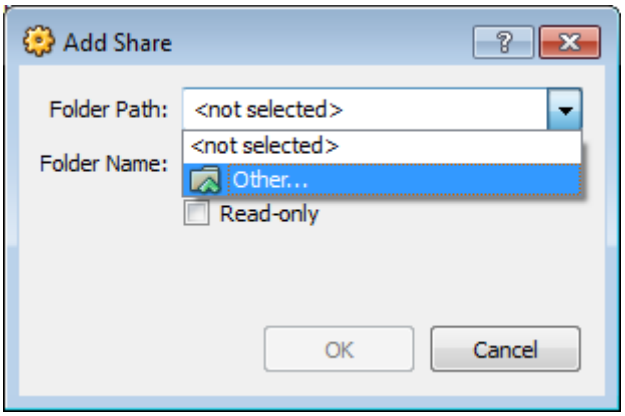
این امکان وجود دارد که روی سیستم عامل واقعی، چندین کانکشن Virtual Box وجود داشته باشد که در این صورت، پس از انتخاب گزینه Host-Only Adapter، بایستی کانکشن مورد نظر را نیز انتخاب نمایید.



یکی دیگر از امکانات Virtual Box، امکان به اشتراک گذاری پوشه ای خاص بین سیستم عامل واقعی و سیستم عامل مجازی می باشد تا بتوان برخی فایل ها را به راحتی بین هر دو سیستم عامل منتقل نمود. بدین منظور، ابتدا یـک پوشـه در سیسـتم عامل واقعی بسازید. سپس در بخش تنظیمات وارد قسمت Shared Folders شوید.

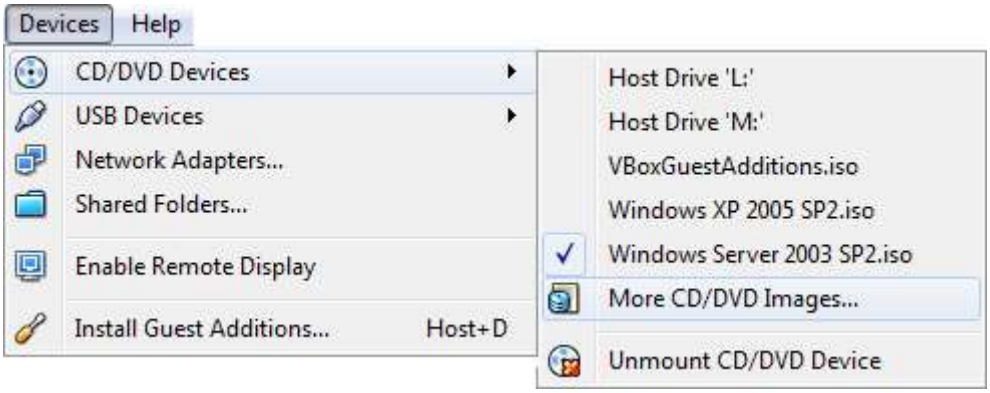


برای افزودن پوشه ای جدید برای اشتراک گذاری، روی دکمه کلیک نمایید. در صفحه باز شده، گزینـه Other را انتخـاب نموده و سپس پوشه مورد نظر را جهت به اشتراک گذاری انتخاب نمایید. این پوشه به صورت یک درایو Map شده در سیستم عامل مجازی نمایش داد می شود.



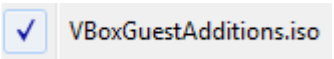
سپس سی دی ویندوز را در سی دی رام قرار داده و سپس سیستم عامل مجازی را انتخاب نموده و روی دکمه Start کلیک کنید.

صبر نمایید تا عملیات نصب سیستم عامل مجازی خاتمه یابد و سیستم عامل مجازی بالا بیاید. پس از بالا آمدن سیستم عامل مجازی، در هر لحظه امکان تغییر سی دی رام وجود دارد. حتی می توان یک فایل Image را به عنوان یک سی دی رام به سیستم عامل مجازی معرفی نمود. برای انجام این کار، در صفحه سیستم عامل مجازی، از منوی Devices، و قسمت CD/DVD Devices، یکی از سی دی رام های موجود را انتخاب کنید. اگر قصد دارید که یک فایل Image را به عنوان سی دی رام معرفی نمایید، گزینه More CD/DVD Images را انتخاب نمایید.

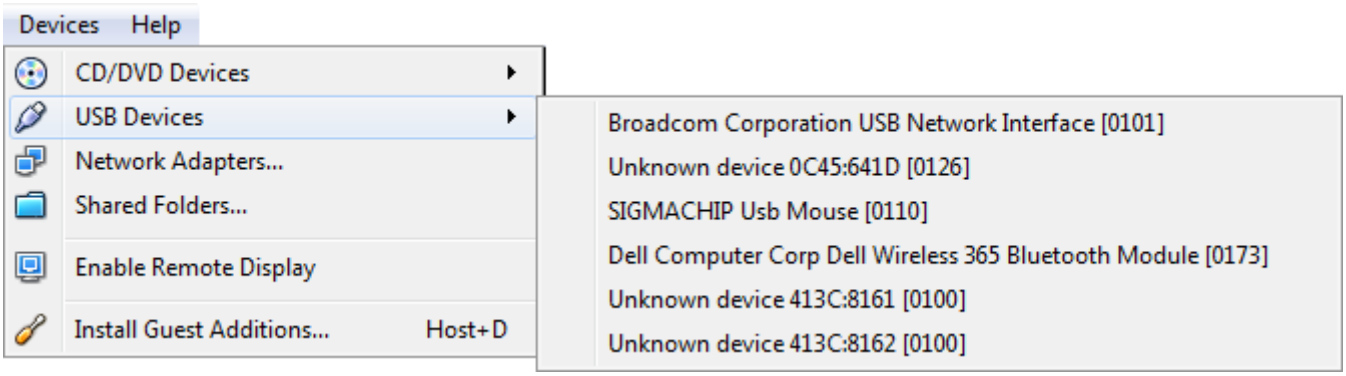


در صفحه باز شده، می توانید فایل های Imageای که تا کنون استفاده کرده اید را مشاهده نمایید. جهت انتخاب فایل Image جدید، روی دکمه Add کلیک نموده و سپس فایل Image را انتخاب کنید. بدین ترتیب محتوای این فایل Image به عنوان سی دی رام در سیستم عامل مجازی نشان داده می شود.

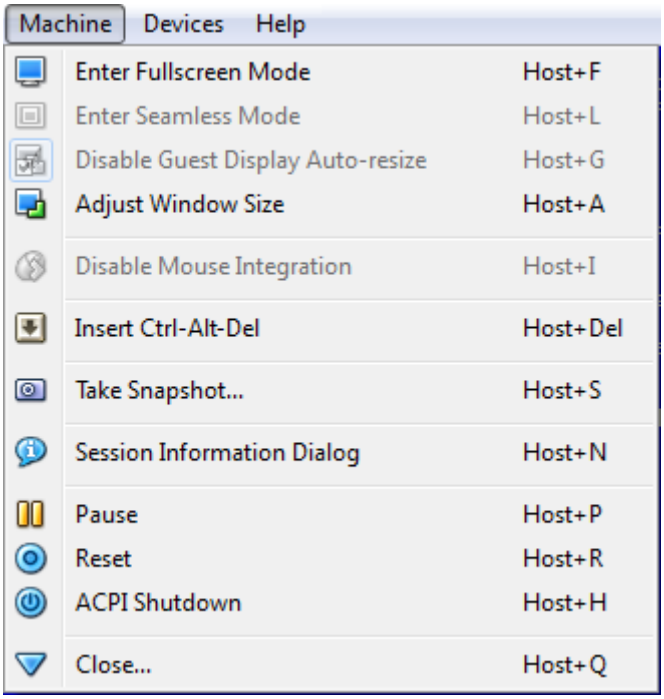
پس از نصب سیستم عامل مجازی و بالا آمدن کامل سیستم عامل، شما نیاز دارید برخی درایور ها را نصب نمایید تا سیستم عامل مجازی بتواند به خوبی و با سرعت بالا کار کند. مثلاً بتواند Full Screen شود. این درایور ها به صورت پیش فرض توسط نرم افزار Virtual Box عرضه شده است. جهت استفاده از آن، از قسمت CD/DVD Devices ➔ Devices، گزینه VBoxGuestAdditions.iso را انتخاب نمایید. محتویات این فایل Image در قالب سی دی رام نمایش داده می شود. محتویات آن را نصب نموده و سیستم عامل مجازی خود را Restart نمایید.



از طریق منوی Devices ➔ USB Devices نیز می توان تجهیزات USB را به سیستم عامل مجازی معرفی نمود.



منوی Machine نیز امکاناتی را نظیر Full Screen و کلید های Ctrl+Alt+Del را در اختیار قرار می دهد. در کلید های میانبر، منظور از کلمه Host، دکمه Ctrl سمت راست می باشد که البته این دکمه قابل تغییر می باشد.



در قسمت پایین پنجره نیز دکمه هایی به ازاء تجهیزات وصل شده، مانند هارد دیسک، آداپتور شبکه و... تعبیه شده است.

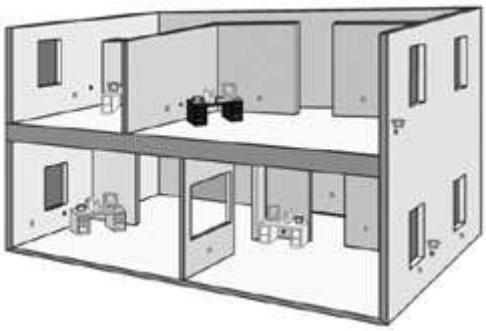
جهت پیاده سازی مناسب مثال های این جزوه، توصیه می شود که روی نرم افزار Virtual Box، دو عدد Windows XP و یک عدد Windows Server 2003 نصب شود.

فصل ۱۰

راه اندازی شبکه Workgroup و نحوه Share کردن داده ها

۱۰-۱- اشتراک گذاری

اگر در محیط کار یا منزل خود با بیش از یک کامپیوتر سروکار دارید، احتمالا به فکر افتاده اید که آن ها را به یکدیگر متصل کرده و یک شبکه کوچک کامپیوتری راه بیندازید.



از طریق یکی از کامپیوتر ها که به اینترنت وصل است، بقیه را نیز به اینترنت متصل کنید؛ از هر یک از کامپیوتر ها به فایل های خود از جمله عکس ها، آهنگ ها و اسناد دسترسی پیدا کنید؛ به بازی هایی بپردازید که به چند بازیکن با چند کامپیوتر نیاز دارند و بالاخره این که خروجی وسایلی چون DVD Player یا وب کم را به سایر کامپیوتر ها ارسال کنید.

در این فصل ضمن معرفی روش های مختلف اتصال کامپیوتر ها به یکدیگر، انجام تنظیمات دستی را برای بهره بردن از حداقل مزایای یک شبکه کامپیوتری به شما نشان می دهیم.

۱۰-۲- روش های اتصال

برای اتصال کامپیوتر هایی که در فاصله ای نه چندان دور از یکدیگر قرار دارند راه های مختلفی وجود دارد که عبارتند از:

۱. سیم کشی Data به صورت تو کار در حین ساخت ساختمان که امروز بسیار متداول است. در این روش همان گونه که برای برق ساختمان از قبل نقشه می کشند و مثلاً جای کلید ها و پریز ها را مشخص می کنند، برای شبکه کامپیوتری هم نقشه کشی و سیم کشی می کنند.
۲. قرار دادن سیم ها در کف اتاق و اتصال کامپیوتر هایی که در یک اتاق قرار دارند.
۳. استفاده از فناوری بی سیم
۴. استفاده از سیم کشی برق داخل ساختمان
۵. استفاده از سیم کشی تلفن داخل ساختمان

هر یک از این روش ها، مزایا و معایب خاص خود را دارند اما برای به اشتراک گذاشتن چاپگر، فایل ها و اینترنت باید کامپیوتر ها را به نحو صحیح و مناسبی تنظیم و آماده کنید و فرق نمی کند که کدام روش را انتخاب کرده باشید. به همین دلیل کار را از همین نقطه شروع می کنیم از آنجا که ویندوز XP، پر استفاده ترین ویندوز در منازل و دفاتر کوچک هست، نحوه اشتراک گذاری منابع در این ویندوز را مورد بحث قرار می دهیم. هر چند در مورد سایر ویندوز ها مفاهیم تغییر نمی کند.

۱۰-۳- مراحل انجام کار

برای راه اندازی شبکه در منزل خود این سه کار را باید انجام دهیم:

۱- انتخاب فناوری مناسب شبکه مورد نظر، که در این فصل، استاندارد مورد نظر، اترنت است.

۲- خرید و نصب سخت افزار مناسب این کار، که اصلی ترین آن ها کارت شبکه برای هر یک از کامپیوتر های شبکه و یک هاب یا سوئیچ است.

۳- آماده سازی سیستم ها به نحوی که بتوانند همدیگر را ببینند و اصطلاحا با یکدیگر صحبت کنند.

از این سه مرحله، گزینه سوم از همه مهم تر است. گزینه اول و دوم را که در فصل های پیشین توضیح دادیم. در واقع ما در این لحظه، فرض می کنیم که شما تجهیزات سخت افزاری مورد نیاز جهت ایجاد یک شبکه محلی را فراهم کرده اید (مثلاً از یک سوئیچ استفاده کرده و آن را پیکربندی نموده و کامپیوتر های خود را به آن متصل کرده اید یا در ساده ترین حالت ۲ کامپیوتر را با یک کابل UTP به صورت مستقیم به هم وصل کرده اید). لذا فقط به بررسی تنظیمات نرم افزاری می پردازیم.

ویندوز XP قسمتی به نام Network Setup Wizard دارد که تنظیمات شبکه را برای شما انجام میدهد (این قسمت در Control Panel قرار دارد). به غیر از حالت، این متخصصان هستند که در ازاء دریافت دستمزد، شبکه شما را در محل راه می اندازند. نام گذاری کامپیوتر ها، به اشتراک گذاشتن چاپگر ها، فایل ها و اتصالات اینترنتی، اساسی ترین کارهایی هستند که این افراد برای شما انجام می دهند. اما اگر با مشکلی مواجه بشوید یا تنظیمات کامپیوتر تان بهم بخورد، باید بتوانید خودتان شبکه را تنظیم کنید.

کلا بد نیست مفاهیم و اصول راه اندازی یک شبکه کامپیوتری را بدانید تا به هنگام ضرورت خودتان بتوانید دست به کار شوید. به طور کلی کار هایی که باید انجام دهید تا یک شبکه "مرده" را "زنده" کنید و به بهره برداری از آن بپردازید، از این قرار است:

۱. نام گذاری کامپیوتر
۲. دادن آدرس IP
۳. به اشتراک گذاشتن فایل ها
۴. به اشتراک گذاشتن چاپگر

۵. انجام تنظیمات امنیتی
۶. به اشتراک گذاشتن اتصال اینترنت
۷. اتصال یک درایو به پوشه Share شده (Map Network Drive)

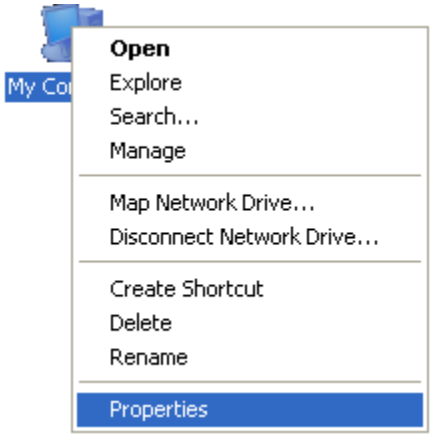
۱۰-۳-۱- نام گذاری کامپیوتر

بعد از نصب سخت افزار های مورد نیاز برای راه اندازی شبکه، نوبت به نصب نرم افزار های آن می رسد. در اولین قدم باید برای تک تک کامپیوتر های موجود در شبکه خود اسمی منحصر به فرد و غیر تکراری انتخاب کنید.

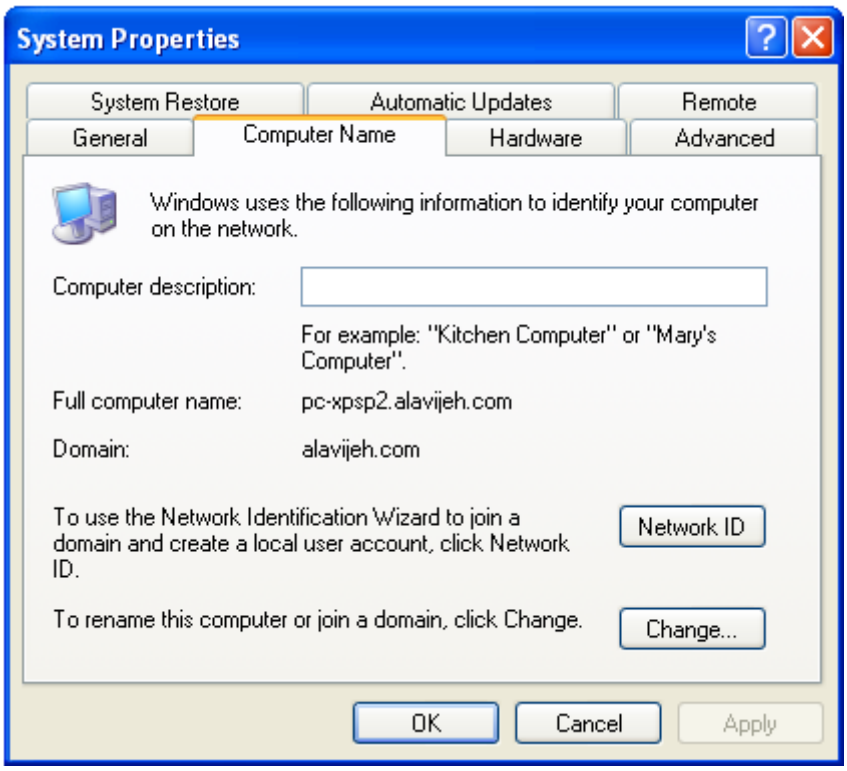
علاوه بر اسم کامپیوتر اسم گروه کاری یا Work Group هم مهم است. تمام کامپیوتر های یک شبکه باید عضو یک گروه کاری باشند.

برای نام گذاری کامپیوتر در ویندوز XP این مراحل را دنبال کنید:

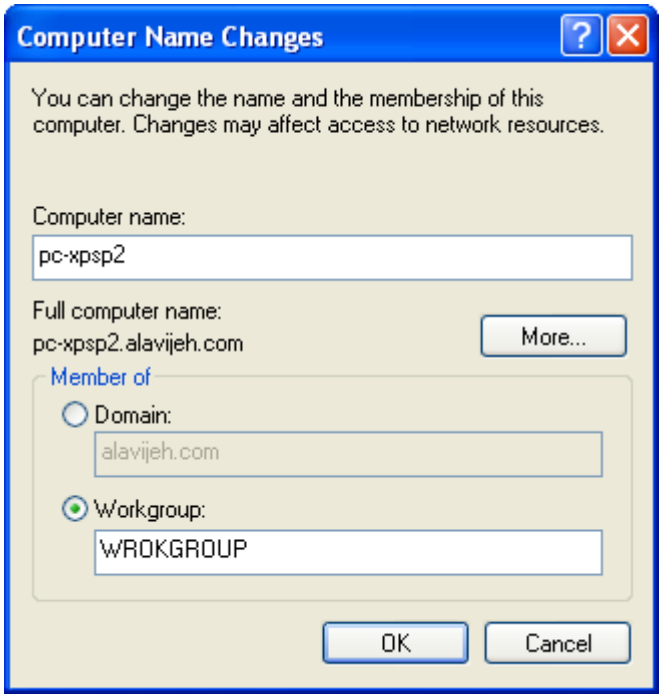
۱- بر روی My Computer راست کلیک کرده و گزینه Properties را انتخاب نمایید.



۲- در کادر محاوره ظاهر شده صفحه Computer Name را انتخاب کنید.



۳- بر روی دکمه Change کلیک کنید تا صفحه زیر باز شود.



همان طور که ملاحظه می کنید کامپیوتر یک اسم کامل دارد و یک گروه کاری.

۴- در کادر اول اسمی را تایپ کنید که می خواهید به کامپیوتر تان اختصاص دهید. این اسم هر چیزی می تواند باشد، فقط نباید تکراری باشد. مثلاً اسم کامپیوتر اول را PC1 بگذارید.

۵- در کادر دوم اسمی را که می خواهید به گروه کاری خود اختصاص دهید وارد کنید. مثلاً My office یا My Home یا هر چیز دیگر. حتی خود Work Group هم بد نیست.

۶- در پایان OK و دوباره OK را بزنید. اگر ویندوز خواست Restart کند، قبول کنید.

۱۰-۳-۲- آدرس IP

آدرس IP نشانی هر کامپیوتر در شبکه است. کامپیوتر از طریق این نشانی است که یکدیگر را در شبکه پیدا می کنند.

در هر شبکه آدرس IP هر کامپیوتر باید منحصر به فرد و غیر تکراری باشد.

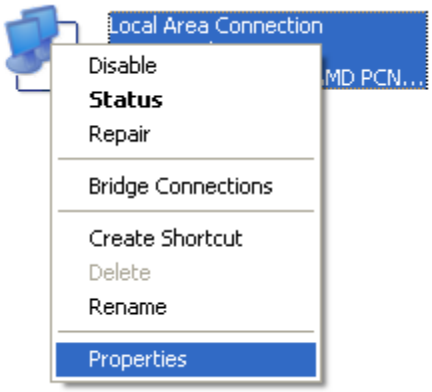
سپس به تعیین آدرس IP و آدرس Subnet Mask می پردازیم که توضیحات آن را در فصول قبل ارائه کردیم.

در یک شبکه کوچک، برای تمام کامپیوتر ها، سعی می کنیم کلاس آدرس IP را Class A در نظر بگیریم. لذا سه قسمت اول آدرس IP را یکسان می گیریم و فقط قسمت چهارم را برای هر کامپیوتر عدد متفاوتی را در نظر می گیریم.

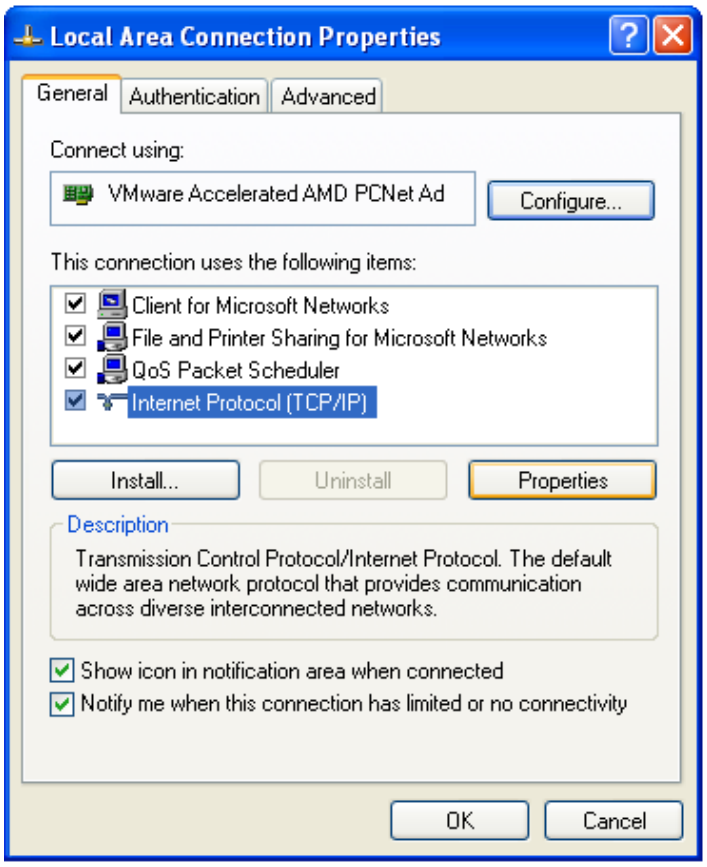
مثلاً در کامپیوتر اول آدرس ۱۹۲.۱۶۸.۰.۱ و برای کامپیوتر دوم آدرس ۱۹۲.۱۶۸.۰.۲ را می نویسیم و به همین ترتیب در بقیه کامپیوتر ها قسمت چهارم آدرس IP را عدد متفاوتی را می دهیم.

۱- Control Panel را باز کرده و Network Connections را انتخاب کنید

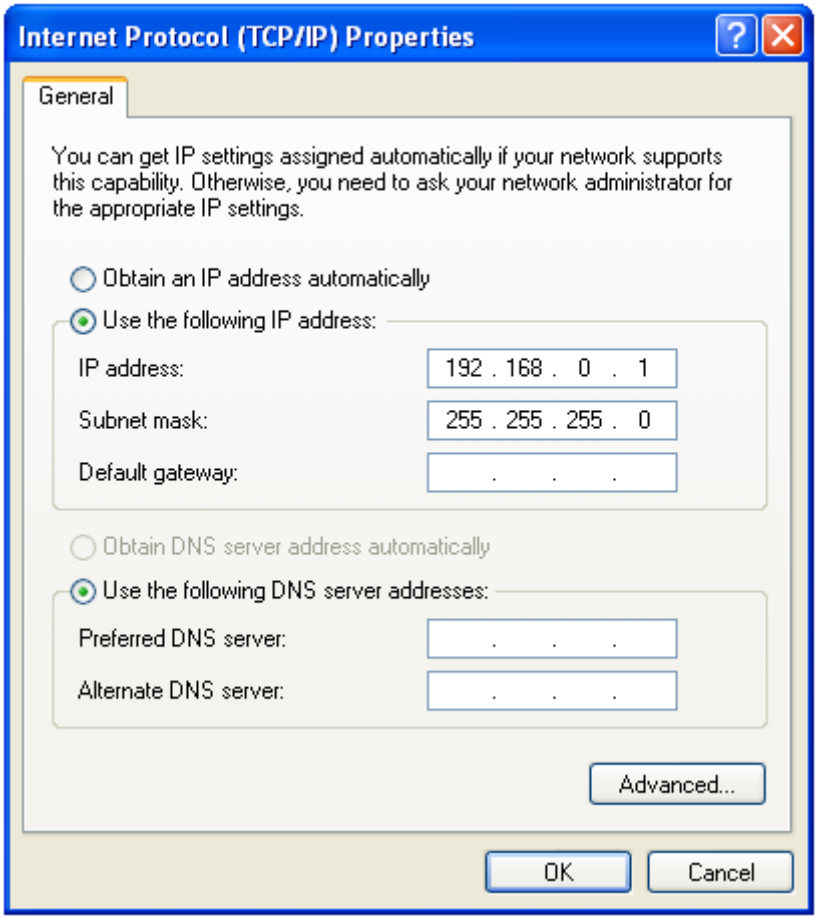
۲- بر روی آیکون Local area connection کلیک راست کرده و گزینه Properties را انتخاب کنید.



۳- در پنجره بعدی روی Internet Protocol (TCP/IP) کلیک کرده و کلید Properties را کلیک نماید.



۴- طبق توضیحات فوق IP مورد نظر و سایر اطلاعات را وارد کنید.



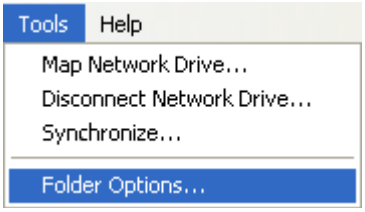
۲- دکمه OK و دوباره OK را بزنید.

بعد از این که به همین ترتیب به بقیه کامپیوتر ها هم آدرسIP دادید، نوبت به Share کردن فایل ها و پوشه ها می رسد. شبکه ای که نتواند فایل هایش را با دیگران سهیم کند، زیاد به درد نمی خورد. مثلاً می توانید مجموعه فایل های MP3 و موسیقی خود را در یکی از کامپیوتر ها بگذارید و با Share کردن آنها، به بقیه کامپیوتر ها هم اجازه دسترسی بدهید.

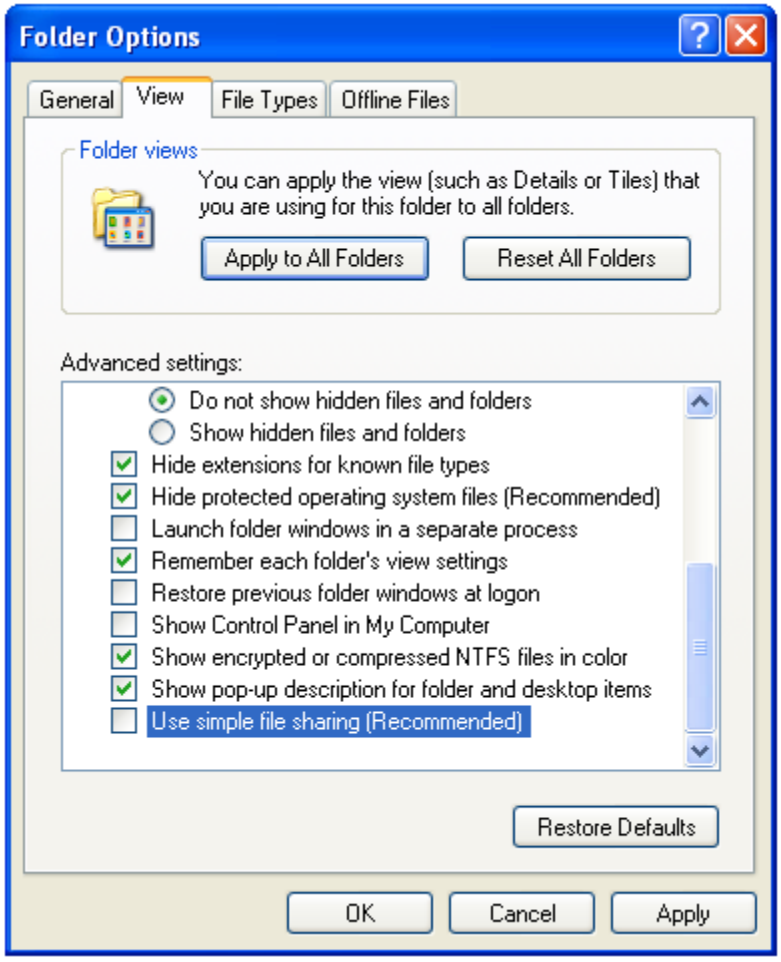
۱۰-۳-۳- به اشتراک گذاشتن فایل ها (File Sharing) و استفاده از آن ها

یکی از کاربردهای اصلی شبکه، به اشتراک گذاشتن فایل ها میان کامپیوتر ها است. این کار در ویندوز، به ویژه ویندوز XP، بسیار آسان است.

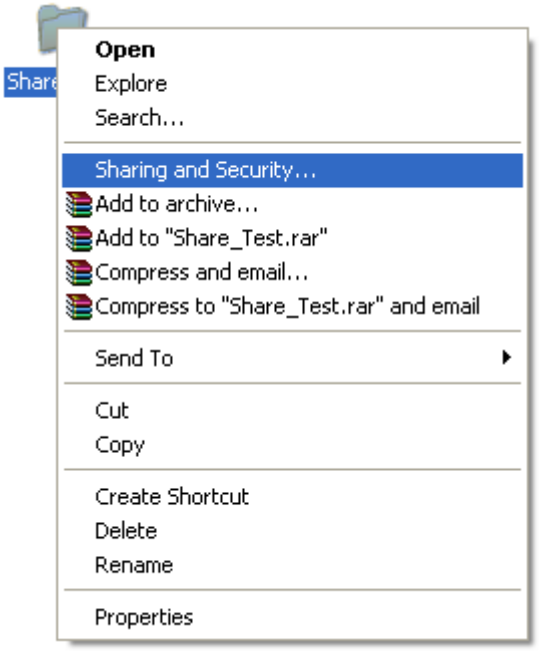
۱- ابتدا وارد My Computer شده، سپس از منوی Tools گزینه Folder Option را انتخاب نمایید.



۲- سپس وارد سربرگ View شده و سپس تیک گزینه آخر یعنی گزینه Use Simple File Sharing را بردارید.



۳- سپس روی پوشه ای که می خواهید آن را Share کنید، راست کلیک کرده و سپس گزینه Sharing and Security را انتخاب کنید.

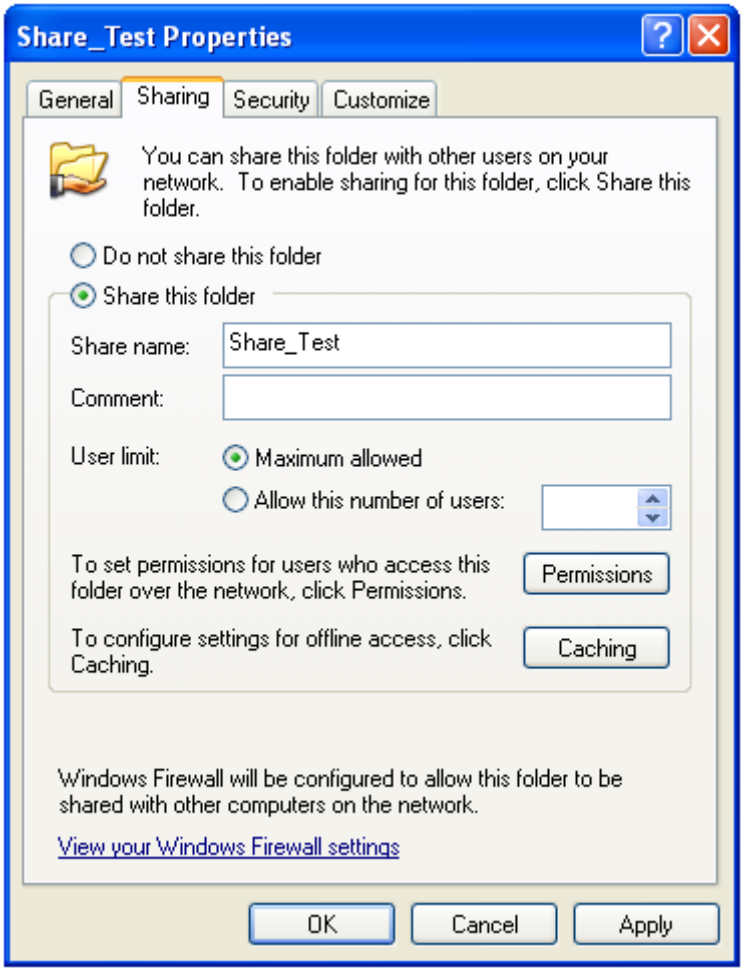


۴- در کادر محاوره ظاهر شده، به صفحه Sharing بروید. حالا گزینه Share This Folder را انتخاب کنید و اسمی را برای پوشه تایپ کنید که می خواهید در شبکه به آن اسم شناخته شود.

وقتی پوشه ای را به اشتراک می گذارید، تمامی کاربران شبکه می توانند پوشه Share شده را ببینند. اگر می خواهید پوشه Share شده را مخفی کنید، هنگام اشتراک گذاری، انتهای نام آن، یک علامت $ قرار دهید (توجه: نام پوشه را تغییر ندهید، بلکه هنگام اشتراک گذاری، در قسمت Share Name، انتهای نام پوشه یک علامت $ بگذارید). در این مثال می شود: Share_Test$

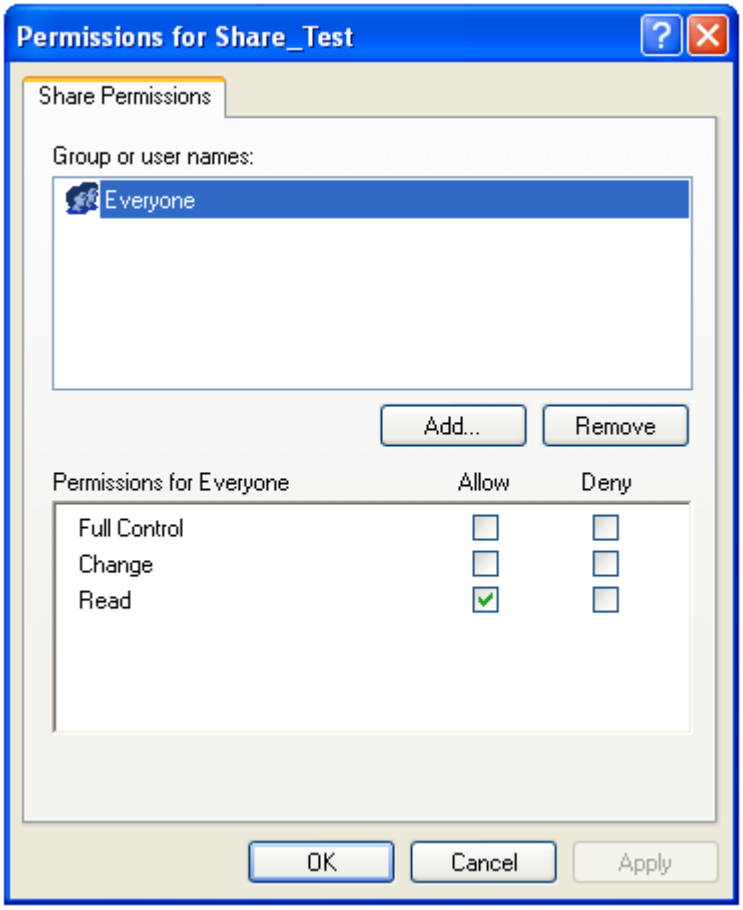
البته به طور پیش فرض در ویندوز XP، برخی قسمت ها به صورت مخفیانه به اشتراک گذاشته شده اند که عبارتند از:

- C$، D$، E$ و... : به اشتراک گذاری ریشه درایو ها
- Admin$: پوشه ویندوز
- IPC$: برای کاربران کاربردی ندارد و برای ارتباط بین برنامه های رایانه در شبکه و مدیریت از راه دور برنامه ها مورد استفاده قرار می گیرد.



۵- در همین صفحه، این قابلیت وجود دارد که تعیین نمایید که به طور همزمان چند نفر در شبکه به این پوشه دسترسی داشته باشند. ایجاد محدودیت روی دسترسی همزمان، تاثیر زیادی در کنترل ترافیک در شبکه های شلوغ دارد. برای تعیین محدودیت دسترسی همزمان، در همین صفحه گزینه Allow this number of users را انتخاب کرده و سپس در جعبه متن روبروی آن، تعداد را وارد نمایید.

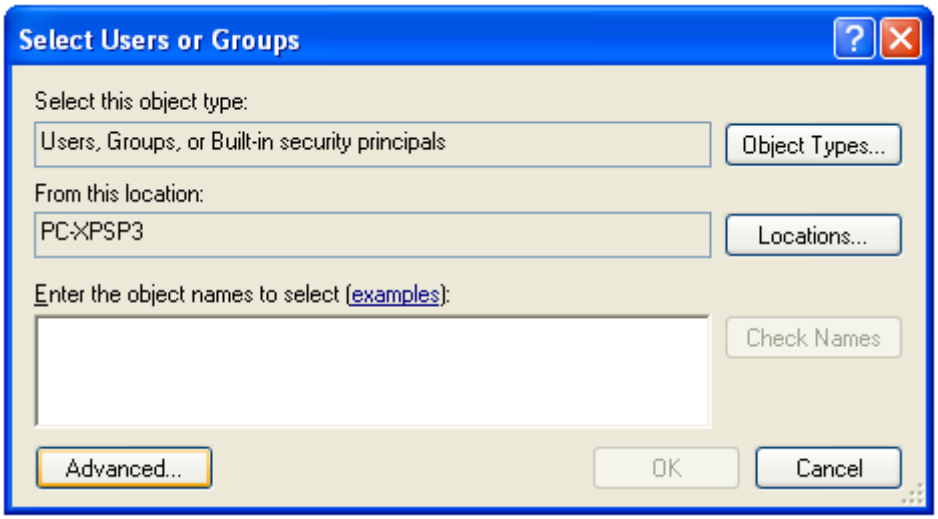
۶- وقتی پوشه ای را در شبکه به اشتراک می گذارید، این اختیار را دارید که نوع دسترسی به آن (و فایل های موجود در آن) را تعیین کنید. این دسترسی می تواند به صورت فقط خواندنی (Read-Only) باشد، یا دسترسی کامل (Full Control) . وقتی دسترسی به صورت فقط خواندنی باشد، کاربر اجازه ندارد پوشه را حذف یا چیزی داخل آن کپی کند، اما می تواند محتوای پوشه را مشاهده و در صورت نیاز آن را در کامپیوتر خود کپی کند. حتی می تواند از همان جا به اجرا یا (مثلاً در مورد موسیقی) به پخش فایل ها بپردازد. در این رابطه در قسمت تنظیم امنیت بیشتر صحبت خواهیم کرد. اما به طور خلاصه، برای تنظیم دسترسی، در همین صفحه روی دکمه Permissions کلیک کنید.



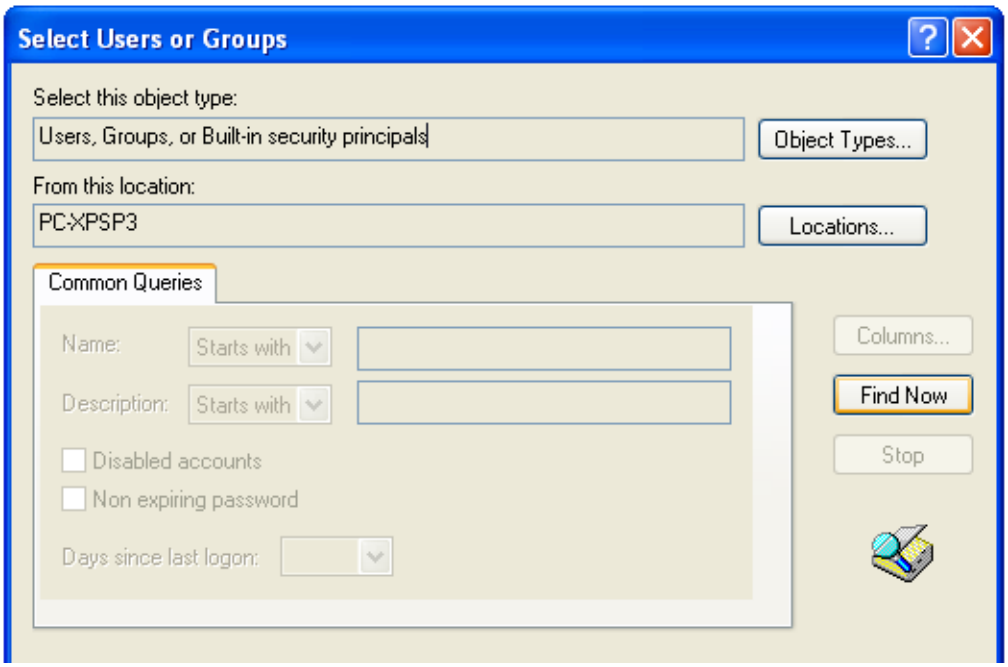
۷- سپس در این صفحه، سطح دسترسی هر کاربر را تعیین نمایید.

۸- می توانید دسترسی کاربر دیگری را نیز تعیین نمایید. برای این کار در همین صفحه روی دکمه Add کلیک کنید.

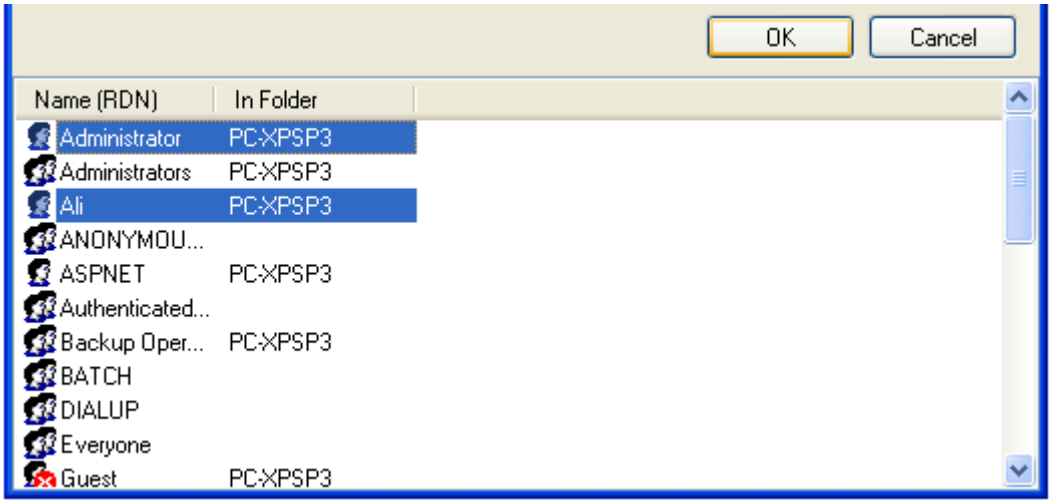
۸- سپس روی دکمه Advanced کلیک نمایید.



۹- سپس در صفحه باز شده، روی دکمه Find Now کلیک کنید تا لیست تمام کاربران و گروه های موجود در کامپیوتر به نمایش در آید.



۱۰- سپس در صفحه باز شده، کاربر (کاربران) یا گروه (گروه های) مورد نظر را انتخاب کنید:



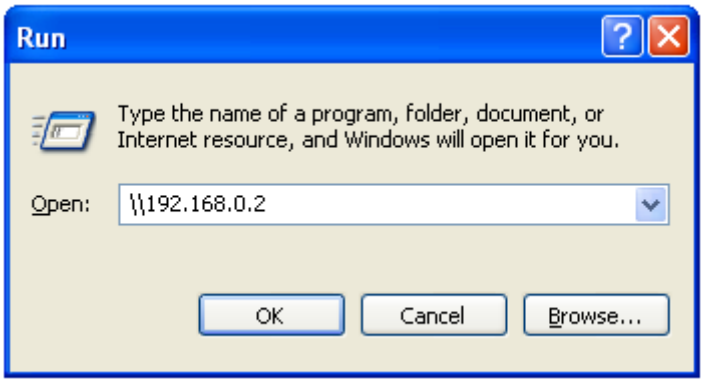
۱۱- سپس دو بار OK نمایید.

۱۲- توجه نمایید که نام Everyone که در صفحه دسترسی ها مشاهده نمودید؛ تمامی کاربران جزء این گروه هستند. لذا در دادن دسترسی به این گروه نهایت دقت را به عمل آورید. زیرا به طور مثال اگر گروه Everyone قابلیت نوشتن داشته باشد، و اگر از کاربری مانند Ali، اجازه نوشتن را بگیرید، بازهم کاربر Ali اجازه نوشتن را دارد.

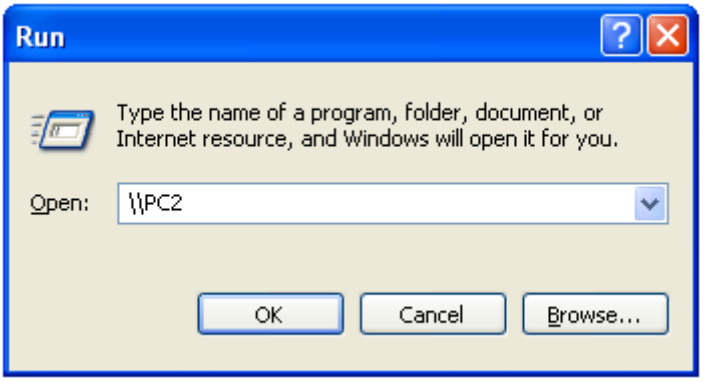
۱۳- برای دسترسی به پوشه ای که به اشتراک گذاشته شده است، از My Computer، لینک My Network Places را کلیک کنید.

۱۴- اگر کسی در کامپیوتر خود پوشه ای را به اشتراک گذاشته باشد، اسم آنها در پنجره شما ظاهر خواهد شد. از این جا به بعد، مثل این است که آن فایل ها و پوشه ها در کامپیوتر خود شما هستند. با دوبار کلیک روی اسم یک پوشه، می توانید محتوای آن را مشاهده کنید. اگر بخواهید می توانید فایل یا پوشه را به کامپیوتر خودتان منتقل کنید. و اگر اجازه داشته باشید، می توانید فایلی را حذف یا Rename کنید.

۱۵- البته راه دیگری نیز برای اتصال به دیگر کامپیوتر ها دارید و آن اینکه ابتدا وارد Run شده و ابتدا علامت \\ نوشته و سپس **اسم کامپیوتر یا آدرس IP** کامپیوتر مقصد را وارد نمایید.



یا



۱۰-۳-۴- به اشتراک گذاشتن چاپگر

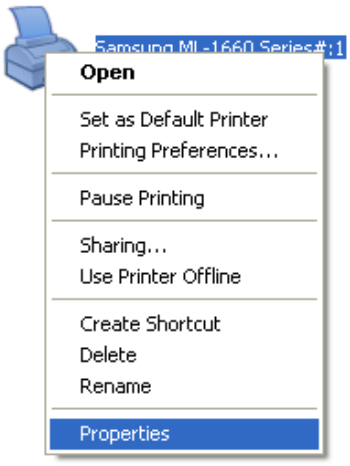
ابتدا با برخی از مفاهیم به اشتراک گذاری چاپگر آشنا می شویم:

- **Print Server**: به سرویس دهنده ای گفته می شود که یک چاپگر در آن نصب و به اشتراک گذاشته می شود.
- **Print Queue**: به کارهای چاپی که در یک چاپگر منتظر چاپ شدن می باشند، گفته می شود.
- **Print Job**: به سندی که برای چاپ به یک چاپگر فرستاده می شود، اطلاق می گردد.

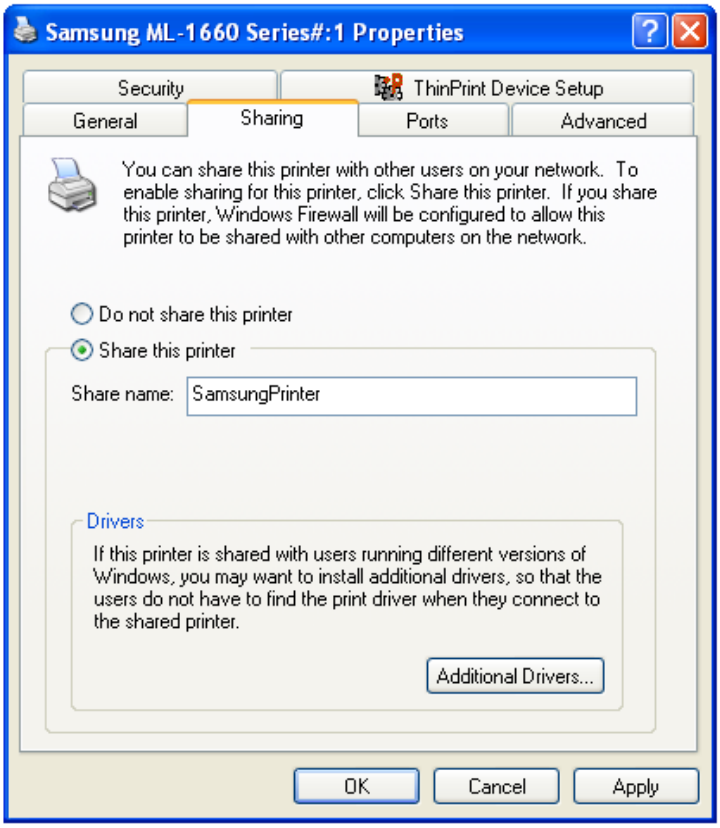
Share کردن چاپگر در ویندوز XP بسیار آسان است:

۱- از منوی استارت، گزینه Printers and Faxes را کلیک کنید.

۲- با کلیک راست روی آیکون چاپگری که قصد Share کردن آن را دارید، گزینه Properties را برگزینید.

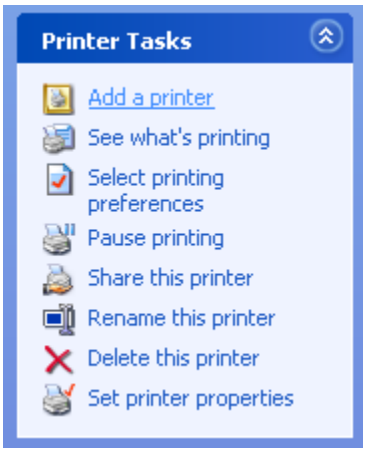


۳- در کادر محاوره ظاهر شده، به صفحه Sharing رفته و گزینه Share this printer را علامت بزنید.

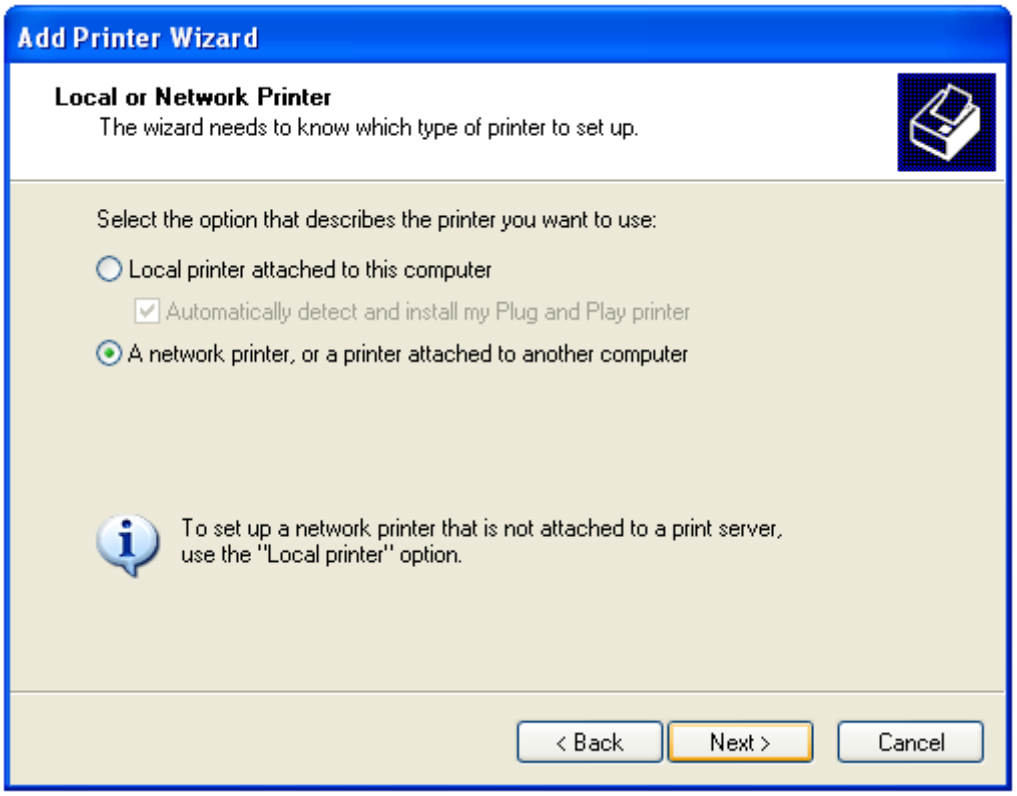


۴- بعد از دادن یک اسم مناسب برای چاپگر خود، دکمه OK را کلیک کنید.

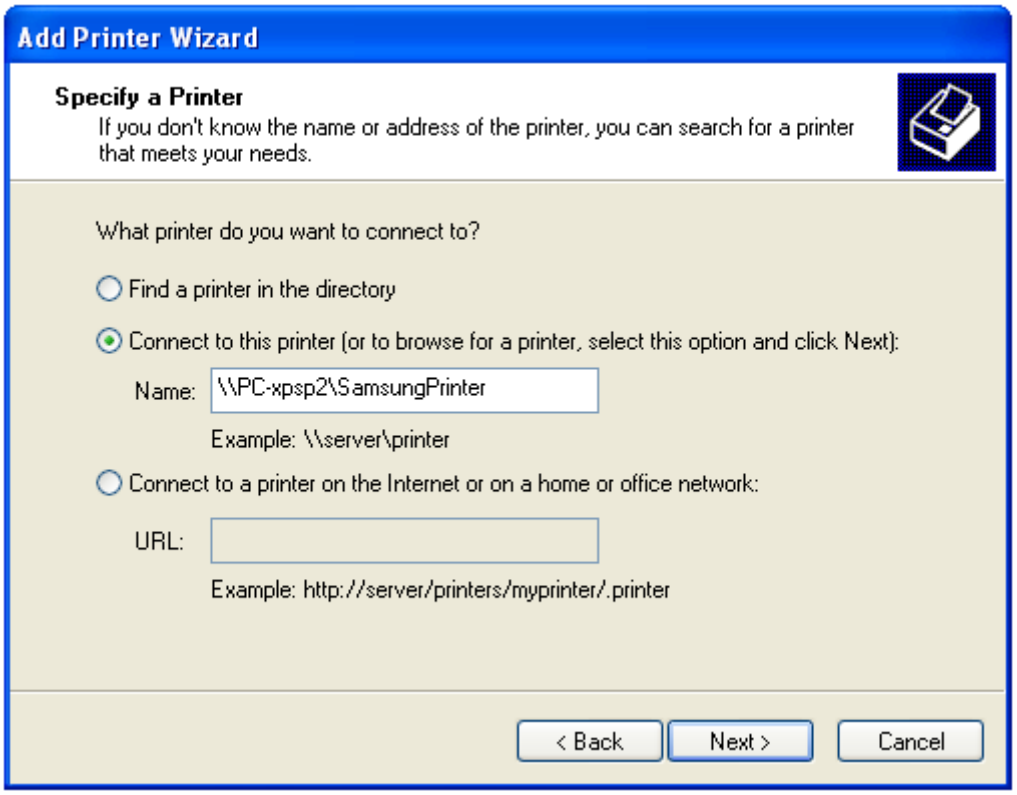
حالا اگر بخواهید از کامپیوتر خود به چاپگری دسترسی پیدا کنید که در شبکه Share شده است، باید به پنجره Printers and Faxes بروید و از ستون سمت چپ، Add a new printer را انتخاب کنید.



ویزاردی شروع به کار می کند که در یک مرحله از آن سؤال می شود که آیا چاپگر به کامپیوتر خودتان متصل است یا جزء چاپگر های شبکه می باشد. شما باید گزینه مربوط به چاپگر شبکه را انتخاب و سپس Next را بزنید.



بعد در شبکه جستجو کنید و چاپگر مورد نظر را پیدا کنید. پس از نصب چاپگر، می توانید به چاپ اسناد خود بپردازید. درست مثل این که چاپگر به کامپیوتر خودتان متصل است.



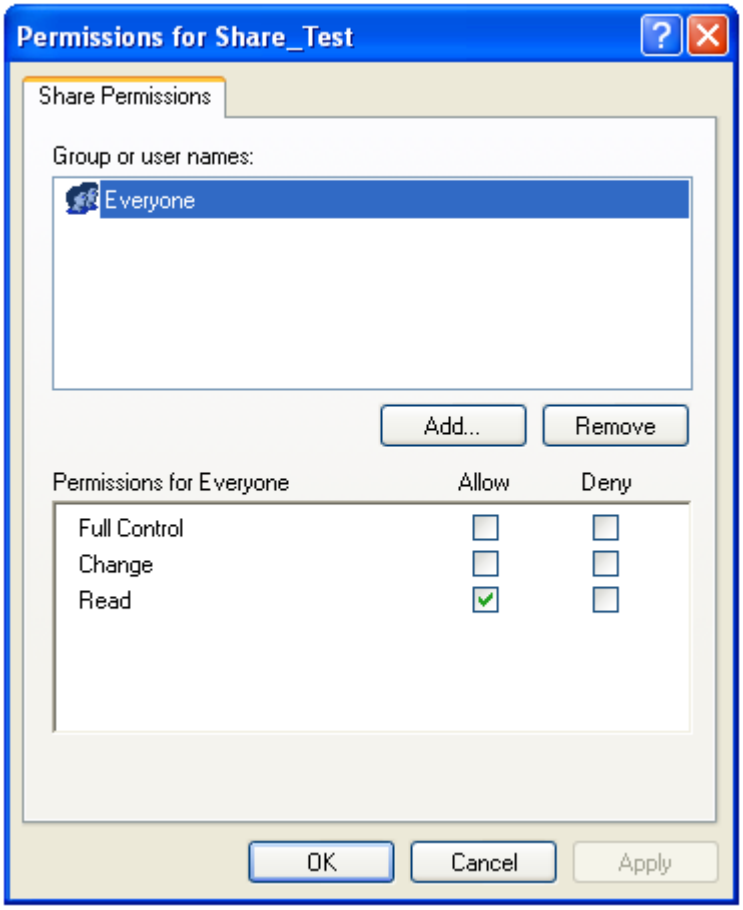
۱۰-۳-۵- تنظیمات امنیتی

منظور از تنظیمات امنیتی تعیین سطح دسترسی است که یک کاربر از راه دور می تواند روی یک فایل یا پوشه Share شده داشته باشد. این کار در دو حالت اصلی "خواندن" و " نوشتن " می تواند باشد. وقتی می گوییم خواندن، یعنی کاربر می تواند

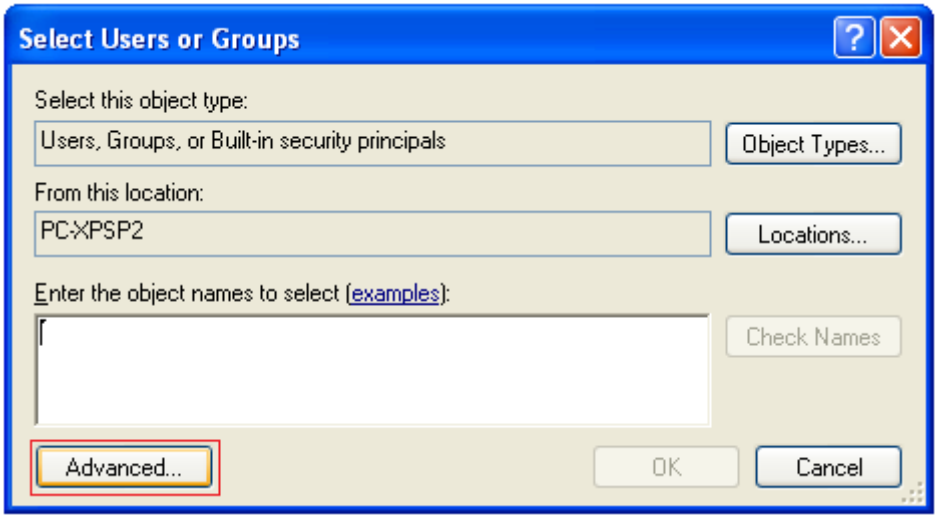
محتوای پوشه را ببینند، فایل های آن را باز، اجرا، پخش یا مشاهده کند، و در صورت نیاز آن ها را به کامپیوتر خود کپی کنـد. اما نوشتن، یعنی این که کاربر می تواند فایل های خود را داخل آن پوشه کپی کند، در صورت لزوم فایل یا تمام پوشه را حذف کند، یا اسم فایل ها یا پوشه را تغییر دهد.

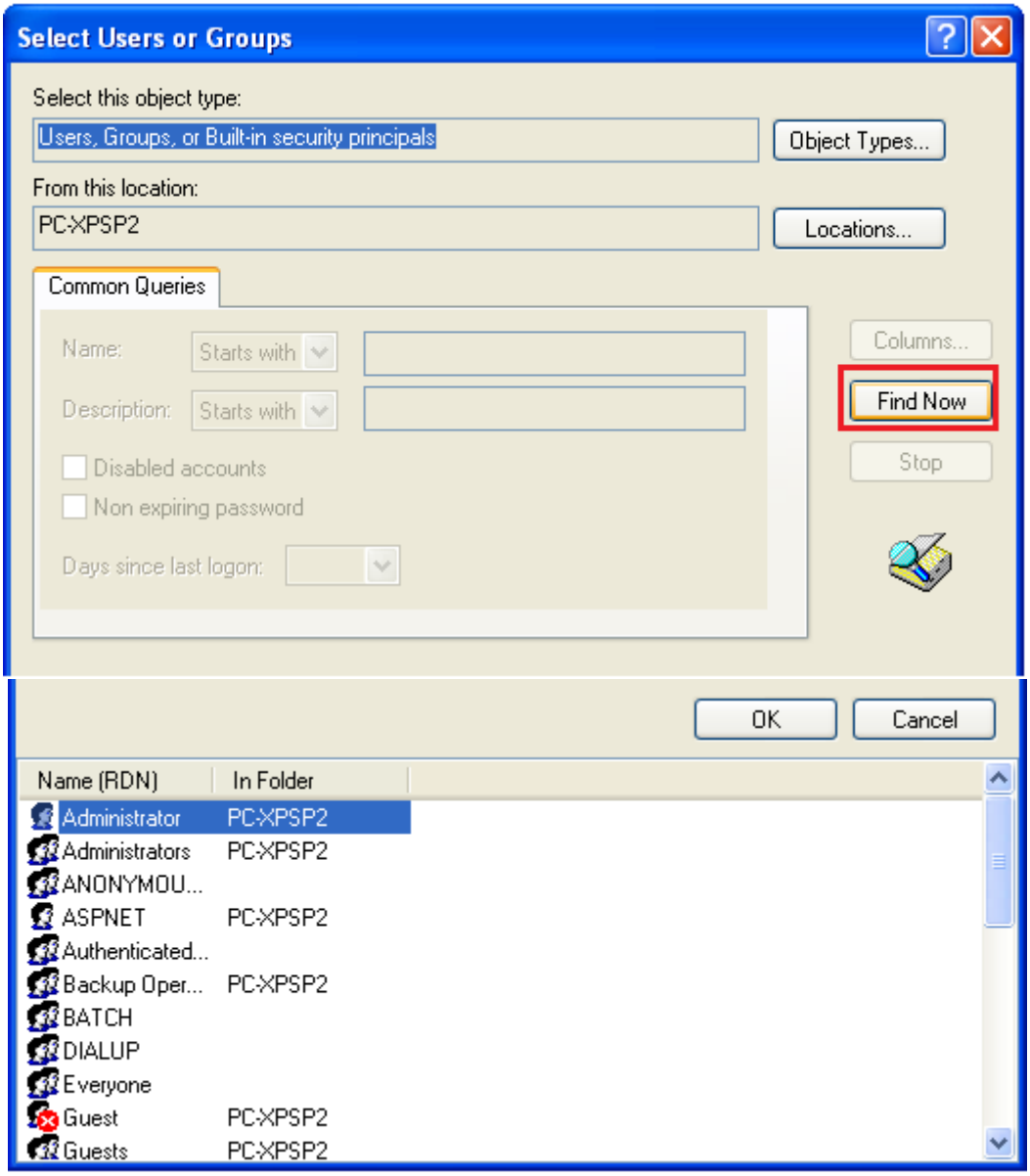
این کارها در ویندوز اکس پی به صورت کاملاً تفکیک شده و جزء به جزء قابل تنظیم هسـتند. مـثلاً اجـازه "دیـدن محتـوای پوشه" از اجازه "اجرای فایل های پوشه" کاملاً تفکیک شده اند، در حالی که عملاً هر دو این کارها جزو "خوانـدن" محسـوب می شوند.

اگر در کادر محاوره ای مربوط به Share کردن پوشه، روی دکمه Permissions کلیک کنید، کادر محاوره دیگـری ظـاهر مـی شود. در این حالت، گزینه هایFull Control، Change و Read را می بینید که هر کدام می تواننـد پذیرفتـه (Allow) یـا رد (Deny) بشوند. به طور پیش فرض، فقط گزینه Read پذیرفته است، که یعنی کاربران فقط اجازه دیدن و استفاده از فایل ها را دارند، نه چیز دیگر.



اگر دقت کرده باشید، در کادر محاوره Permissions، فهرستی از کاربران ارائه شده است. در این شکل شما Everyone را مـی بینید که دسترسی وی Read تعیین شده است. یعنی هر کس که این پوشه Share شده را بخواهد، فقط می تواند آن را ببیند و استفاده کند. ولی شاید بخواهید برای کاربران مختلف دسترسی های متفاوت تعریف کنید. مثلاً کـاربر Administrator مـی تواند دسترسی کامل داشته باشد. برای این منظور، با کلیک روی دکمه Add فهرستی از کاربران تعریـف شـده در سیسـتم را خواهید دید. کاربر یا گروه کاربری مورد نظر خود را انتخاب و OK کنید. حالا می توانید برای این کـاربر، دسترسـی متفـاوتی تعریف کنید.





در اینصورت، هنگام اتصال از دیگر کامپیوتر ها به کامپیوتر شما، بایستی یک Username و Password وارد کرد که در اینصورت، شما دسترسی های Username وارد شده را خواهید داشت.

۱۰-۳-۶- به اشتراک گذاشتن اتصال اینترنت

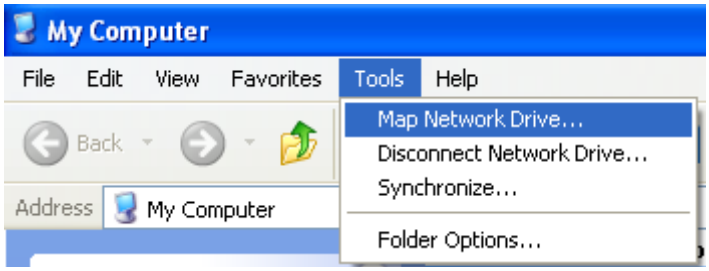
یکی دیگر از منابعی که می توان با اشتراک گذاشت، اتصالات اینترنت می باشد. از آنجا که این بحث مفصل می باشد، آن را در یک فصل جداگانه قرار داده ایم. برای کسب اطلاعات بیشتر به فصل "*به اشتراک گذاشتن اتصال اینترنت*" مراجعه فرمایید.

۱۰-۳-۷- اتصال یک درایو به پوشه Share شده (Map Network Drive)

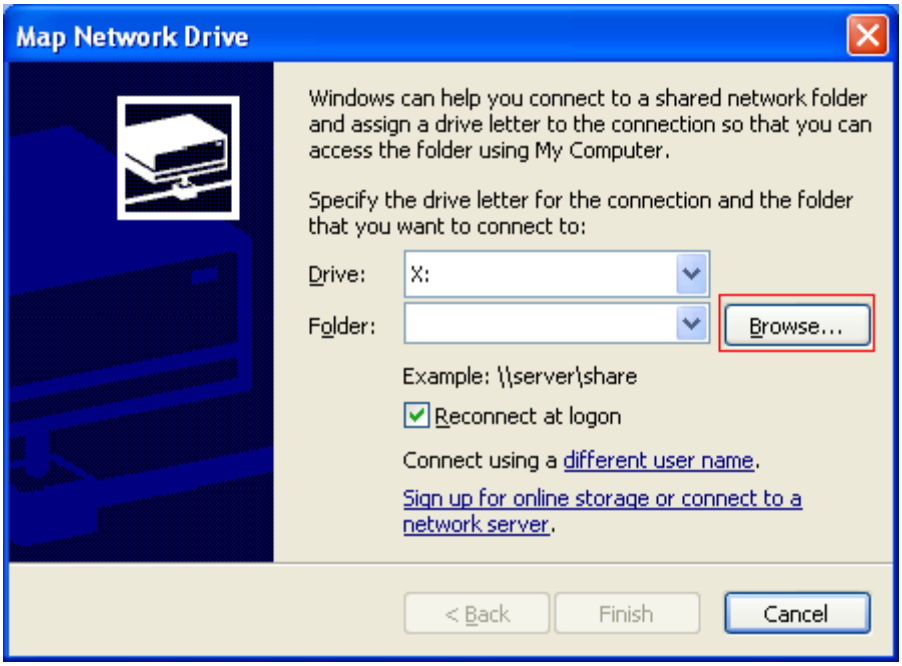
فرض کنید که شما هر روز به پوشه ای نیاز دارید که این پوشه در کامپیوتری دیگر قرار دارد و برای دسترسی به آن نیاز دارید که از طریق Run ابتدا آدرس کامپیوتر مقصد را وارد کرده، سپس پوشه مورد نظر را پیدا کرده، وارد آن شده و از آن استفاده کنید. اما راه ساده تری نیز وجود دارد و آن اینکه در ویندوز این قابلیت وجود دارد که در My Computer یک درایو مجازی بسازید (مثل H:\)، سپس آن را به پوشه Share شده در شبکه Mount کنید، یعنی با بازکردن این درایو، محتویات پوشه Share شده را ببینید. بدین منظور ابتدا در کامپیوتر مقصد یک پوشه ساخته و آن را Share کنید.

سپس در این پوشه یک فایل متنی ایجاد کنید.

حال به کامپیوتر خود رفته و از منوی Tools گزینه Map Network Drive را انتخاب کنید.

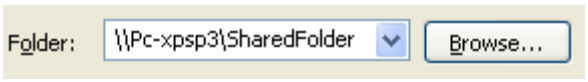


در صفحه باز شده، در قسمت Drive، مشخص کنید که درایو مجازی ساخته شده، با چه اسمی به نمایش درآید؟ (در این مثال X:\)، سپس در قسمت Folder، آدرس یا اسم کامپیوتر مقصد به اضافه نام پوشه Share شده را وارد نمایید. اما برای انتخاب پوشه Share شده به صورت تصویری، روی دکمه Browse کلیک کنید.

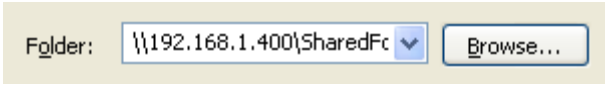


سپس در قسمت Microsoft Windows Network، ابتدا Workgroup مورد نظر، سپس کامپیوتر مورد نظر و سپس پوشه Share شده را انتخاب نمایید.

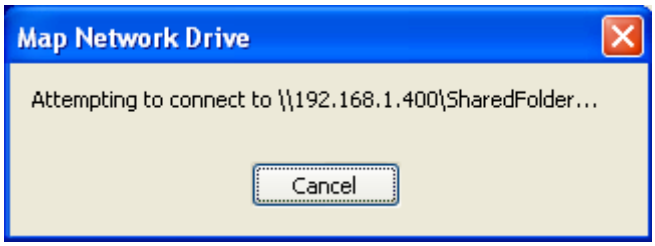
با این کار می بینید که آدرس مورد نظر در بخش Folder قرار می گیرد.



البته می توانید اسم کامپیوتر مقصد، آدرس IP آن را نیز وارد نمایید. توجه کنید که آدرس IP در مواقعی که سیستم ها آدرس IP خود را از DHCP Server می گیرند مناسب نیست.



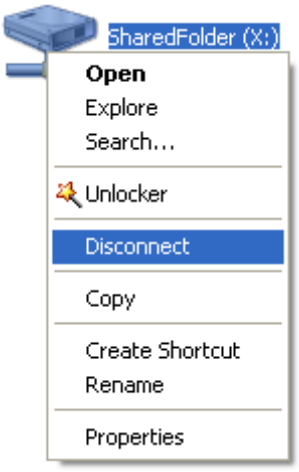
پس از OK کردن صبر کنید تا درایو مورد نظر ساخته شود.



حال اگر وارد My Computer شوید، می بینید که درایو جدید X:\ ساخته شده است.

با بازکردن این درایو، محتویات پوشه Share شده را مشاهده خواهید نمود.

برای حذف این درایو از کامپیوتر خود، روی آن راست کلیک کرده و گزینه Disconnect را انتخاب نمایید.



۱۰-۴- ساختار شبکه

تا اینجا مطالبی را که گفتیم مربوط به زمان بعد از انجام اتصالات فیزیکی یا به اصطلاح کابل کشی شبکه است. حالا ببینیم خود این کابل کشی به چه صورت می تواند انجام شود. همان طور که گفتیم، راه های مختلفی برای وصل کردن کامپیوتر ها به یکدیگر وجود دارد که آسان ترین و در دسترس ترین آن ها اترنت است. لوازم و تجهیزات مورد نیاز برای ساخت یک شبکه اینترنتی می تواند به سادگی اتصال دو کارت شبکه یا به پیچیدگی ارتباط چند روتر و سوئیچ باشد. و در واقع همین انعطاف پذیری این سیستم است که باعث شده شرکت های بزرگ و کوچک به سمت استفاده از آن بروند.

از مزایای سیستم شبکه بندی اینترنت می توان به این موارد اشاره کرد:

۱. سریع ترین تکنولوژی شبکه بندی خانگی است (100 Mbps)
۲. اگر کامپیوتر ها فاصله زیادی از یکدیگر نداشته باشند، هزینه آن بسیار پایین است.
۳. قابل اطمینان است.
۴. نگهداری آن آسان است.
۵. تعداد دستگاه هایی که می توان به شبکه متصل نمود تقریباً نامحدود است.
۶. به لحاظ پشتیبانی و اطلاعات فنی بسیار فراگیر است.

برخی از نقاط منفی این تکنولوژی عبارتند از:

۱. برای وصل کردن بیشتر از دو کامپیوتر به یکدیگر، به تجهیزات اضافی نیاز است.
۲. در صورت نیاز به کابل کشی اضافی و نصب پریز، ممکن است هزینه ها بالا برود.
۳. راه اندازی و تنظیمات اولیه آن می تواند دشوار باشد.
۴. اصطلاحات فنی و تعداد انتخاب ها می تواند گمراه کننده باشد.

۱۰-۵- تجهیزات مورد نیاز

اترنت با سرعت 10 Mbps، 100 Mbps و 1000 Mbps موجود است و بیشتر کارت های شبکه می توانند با هر ۳ سرعت کار کنند، اما امروزه دلیلی ندارد از کارت های 10 Mbps استفاده کنید. و در بسیاری از مواقع تقریباً پیدا کردن کارت های 10 Mbps غیرممکن است. برای وصل کردن کارت های شبکه نیز دو نوع کابل وجود دارد که عبارتند از کابل هم محور (Coaxial) و کابل زوج به هم تابیده (UTP) که اولی تقریباً منسوخ شده و امروزه از UTP در انواع Cat5e، Cat5 و Cat6 استفاده می شود. (کاربرد کابل های Coaxial بیشتر در کابل های آنتن تلویزیون و یا شبکه های BUS است). کابل UTP کابلی است متشکل از ۸ سیم باریک دو به دو به هم تابیده، شبیه به سیم تلفن است. به دو سر این سیم کانکتور یا Jack می

زنند که به RJ-45 معروف است. یک سر این سیم به کارت شبکه کامپیوتر و سر دیگر آن به دستگاهی دیگر وصل می شود؛ مثل سوئیچ، هاب یا کامپیوتر.

تمام کامپیوتر های موجود در یک شبکه، از طریق کابل های UTP به سوئیچ متصل هستند و سوئیچ جای تک تک کامپیوتر ها را می داند. بنابراین وقتی کامپیوتری اطلاعاتی را برای کامپیوتر دیگر ارسال می کند، این ارسال در واقع به واسطه سوئیچ تبادل می شود. یعنی سوئیچ اطلاعات را از کامپیوتر مبدا می گیرد و به کامپیوتر مقصد تحویل می دهد. سوئیچ ها اندازه های مختلفی دارند و این اندازه از روی تعداد پورت شان (یعنی تعداد کامپیوتری که می توان به آنها وصل کرد) مشخص می شود. سوئیچ های ۴ پورتی، ۸ پورتی، ۱۶ پورتی، ۲۴ پورتی و بالاتر در بازار موجود می باشند. برای یک شبکه کوچک خانگی، معمولاً یک سوئیچ ۸ پورتی یا احتمالا ۱۶ پورتی کافی است.

اگر دوست ندارید سیم های شبکه کف اتاق را بپوشانند، می توانید سیم ها را از کانال هایی عبور دهید موسوم به Duct که روی دیوار نصب می شوند. سیم ها داخل داکت قرار می گیرند و در محل استقرار کامپیوتر، از داکت بیرون می آیند و به کارت شبکه کامپیوتر متصل می شوند. اگر بخواهید کار را از این هم تمیزتر انجام دهید، می توانید روی دیوار، پریز های مخصوص شبکه (موسوم به Key Stone) را نصب کنید و با کابل های آماده (موسوم به Patch Cord)، کارت شبکه را به پریز متصل نمایید. بد نیست بدانید که برای وصل کردن فقط دو کامپیوتر به یکدیگر، نیازی به سوئیچ نیست و کافی است از طریق یک کابل UTP مخصوص، موسوم به Cross Over مستقیماً کارت شبکه دو کامپیوتر را به هم وصل کنید.

جدول زیر انواع کابل های UTP را نشان می دهد:

موارد استفاده	سرعت انتقال اطلاعات	گروه
سیستم های قدیمی تلفن، ISDN و مودم	حداکثر تا یک مگابیت در ثانیه	CAT1
شبکه های Token Ring	حداکثر تا چهار مگابیت در ثانیه	CAT2
شبکه های Token ring و 10 BASE-T	حداکثر تا ده مگابیت در ثانیه	CAT3
شبکه های Token Ring	حداکثر تا شانزده مگابیت در ثانیه	CAT4
اترنت (۱۰ مگابیت در ثانیه)، اترنت سریع (۱۰۰ مگابیت در ثانیه) و شبکه های Token Ring (16 مگابیت در ثانیه)	حداکثر تا یکصد مگابیت در ثانیه	CAT5
شبکه های Gigabit Ethernet	حداکثر تا یک هزار مگابیت در ثانیه	CAT5e

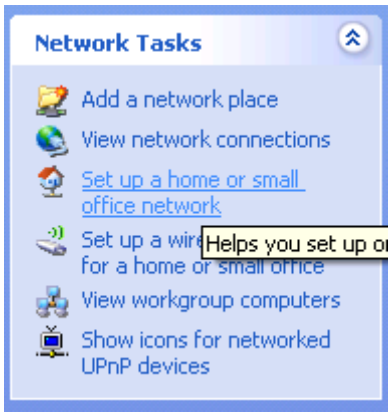
توجه نمایید که اگر برای راه اندازی شبکه خود از سوئیچ (نوع پیشرفته مدیریتی) استفاده نمایید، احتمالا نیاز به پیکربندی آن دارید. اما هاب هیچ تنظیم و مدیریتی نیاز ندارد. فقط کافی است کابل های شبکه را از یک طرف به هاب و از طرف دیگر به کارت شبکه وصل کرده و سپس هاب را روشن نمایید تا چراغ سبز رنگ روی کارت شبکه و چراغ متناظر با پورت مربوطه روی هاب روشن شود.

۱۰-۶- راه اندازی شبکه Workgroup جدید در ویندوز XP

در این قسمت، به آموزش این مبحث می پردازیم که چگونه ویندوز XP را جهت اتصال به یک Workgroup آماده سازیم. ممکن است این سوال برای شما مطرح شود که چرا این مبحث را در انتهای این فصل آورده ایم. موضوعی که مطرح است، این می باشد که ویندوز XP، به صورت خودکار، شبکه های محلی را می شناسد و به آن متصل می شود. اما گاهی مشکلاتی به وجود آمده و دیگر ویندوز XP قادر به متصل شدن به شبکه محلی نخواهد بود و بایستی تنظیمات آن را از ابتدا انجام دهیم. (به همین دلیل افراد حرفه ای رابطه خوبی با محصولات مایکروسافت نداشته و این شرکت را عوام فریب می نامند). شما نیز در صورتی که موفق به راه اندازی شبکه محلی خود نشدید، مراحل زیر را دنبال نمایید.

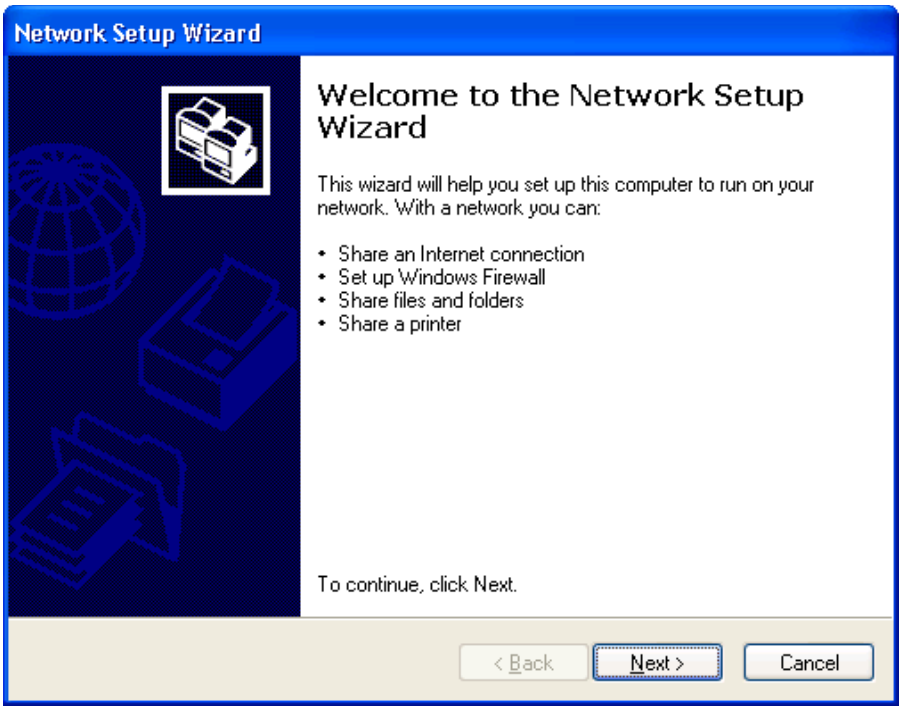
ابتدا وارد My Computer شده و سپس My Network Places را انتخاب نمایید.

سپس در این پنجره گزینه Set up a home or small office network را انتخاب نمایید.

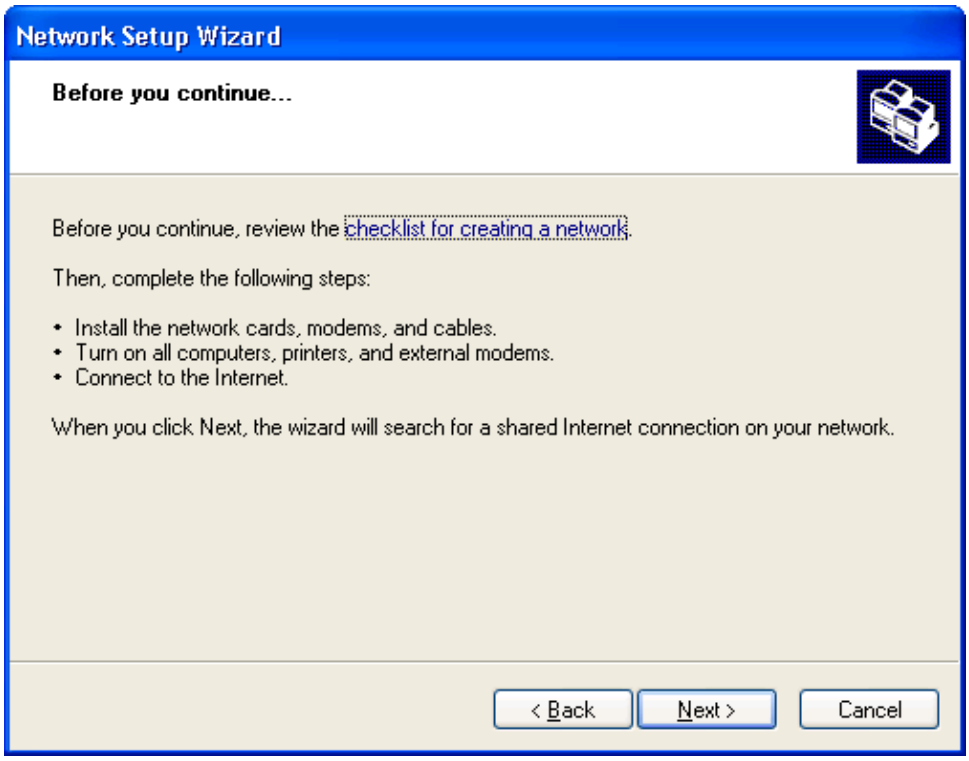


البته راه دیگر برای دسترسی به این قسمت این است که ابتـدا وارد Control Panel شـده و سـپس گزینـه Network Setup Wizard را انتخاب نمایید.

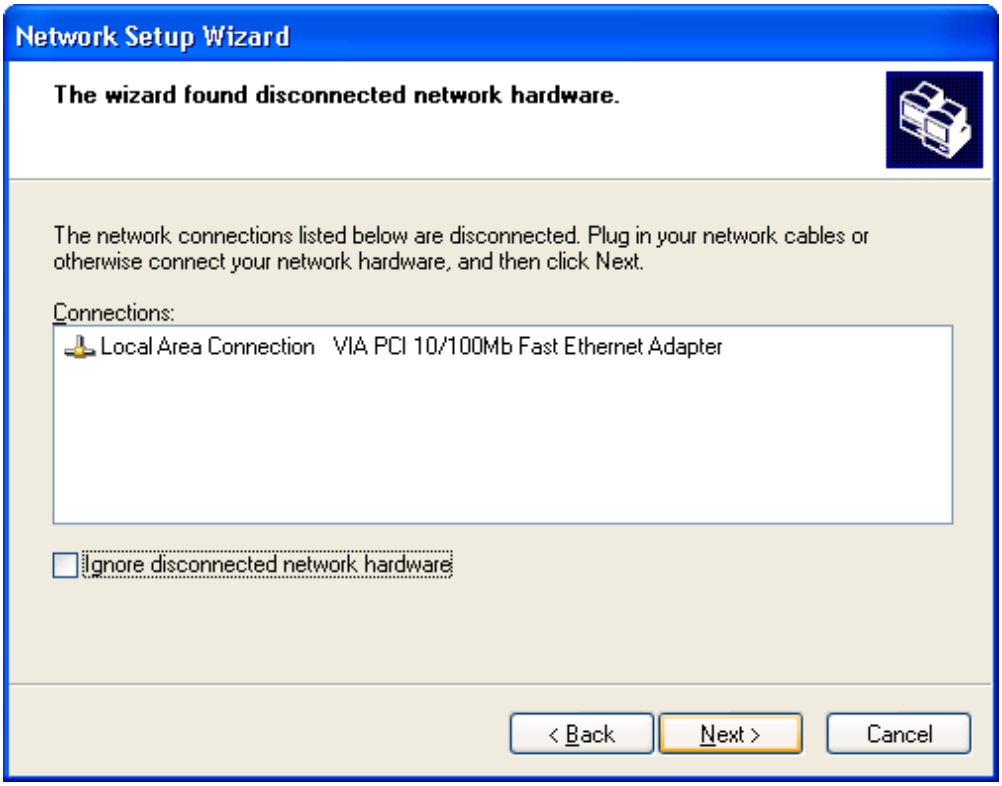
در صفحه باز شده، Next بزنید:



مجددا Next بزنید:

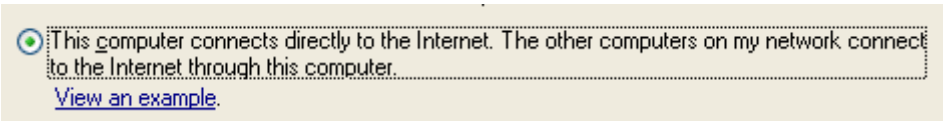


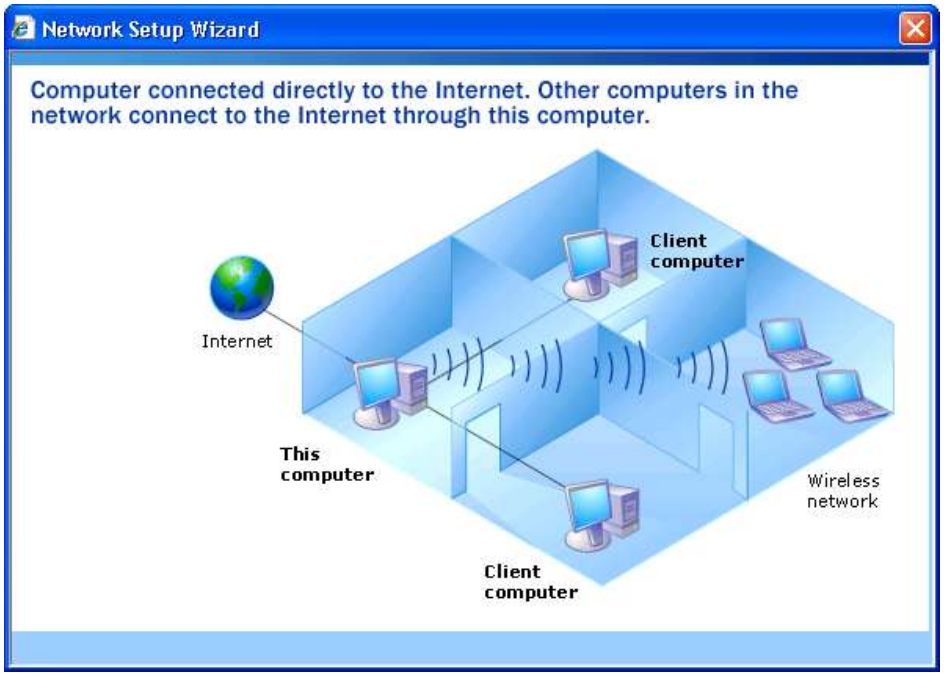
در صفحه باز شده مجددا Next بزنید. در صورتی که سیستم به شما پیام خطـا داد، گزینـه Ignore disconnected network hardware را فعال نموده و سپس Next بزنید.



سپس در صفحه بعد بایستی نوع شبکه داخلی خود را انتخاب کنید. شما ۵ راه دارید، ۲ راه اول را در پنجره بـاز شـده و ۳ راه دیگر را در پنجره بعد از صفحه بعد می توانید ببینید. در کنار هر حالت، گزینه ای تحت عنوان View an example وجود دارد که با انتخاب آن، مثالی مربوط به آن نوع شبکه را مشاهده خواهید کرد. در ادامه ما این ۵ حالت را به تصویر می کشیم:

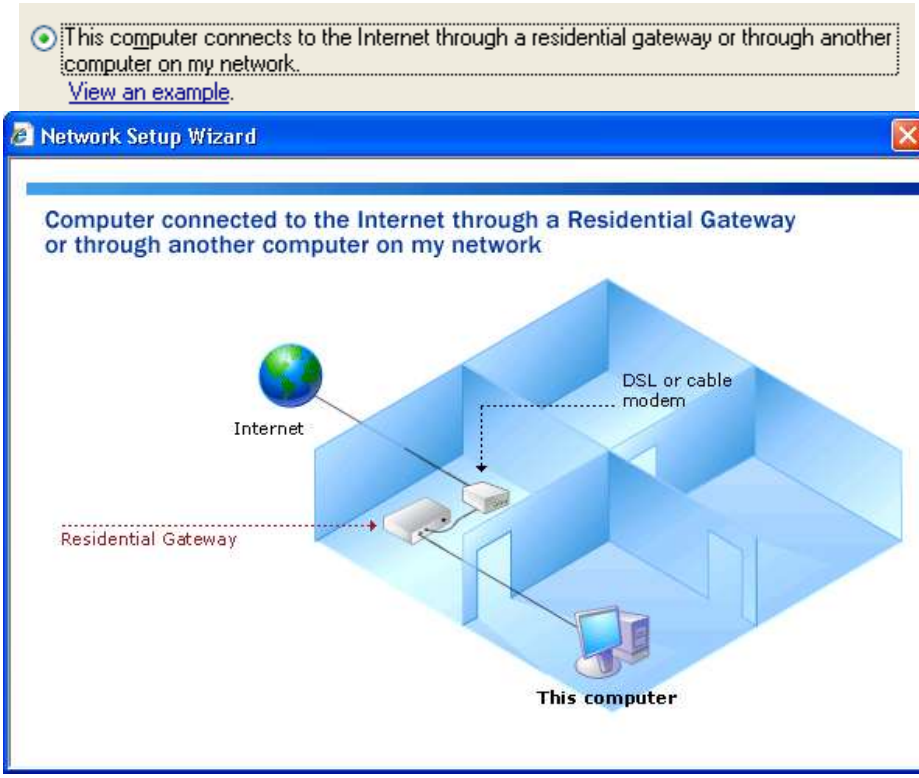
حالت اول





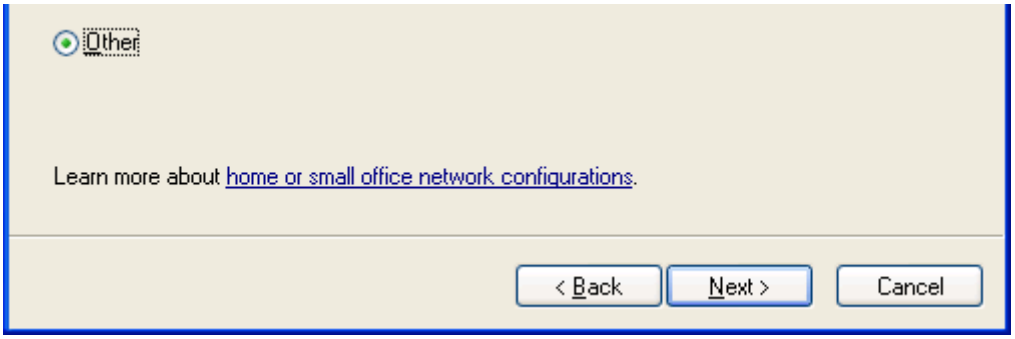
اتصال کامپیوتر شما به اینترنت و سپس به اشتراک گذاری اینترنت.

حالت دوم



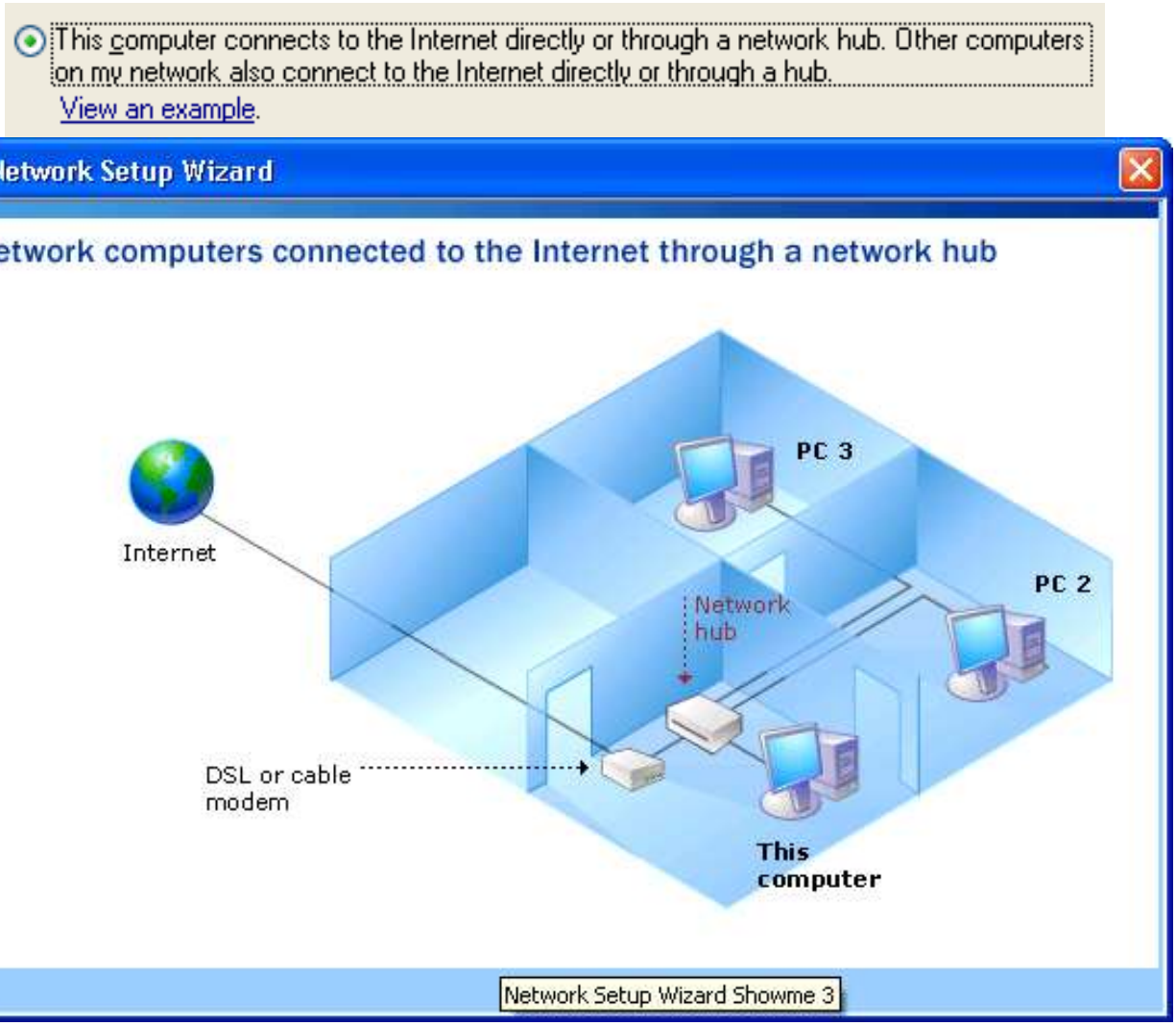
اتصال کامپیوتر شما به یک Gateway و دریافت اینترنت از آن.

در صورتی که هیچ کدام از این دو حالت مد نظر شما نبود، گزینه Other را انتخاب کرده و به مرحله بعد بروید:



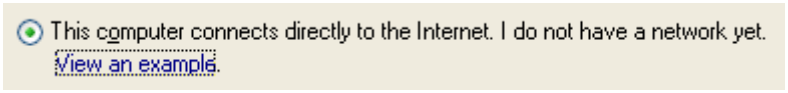
در صفحه باز شده، ۳ حالت دیگر برای انتخاب دارید.

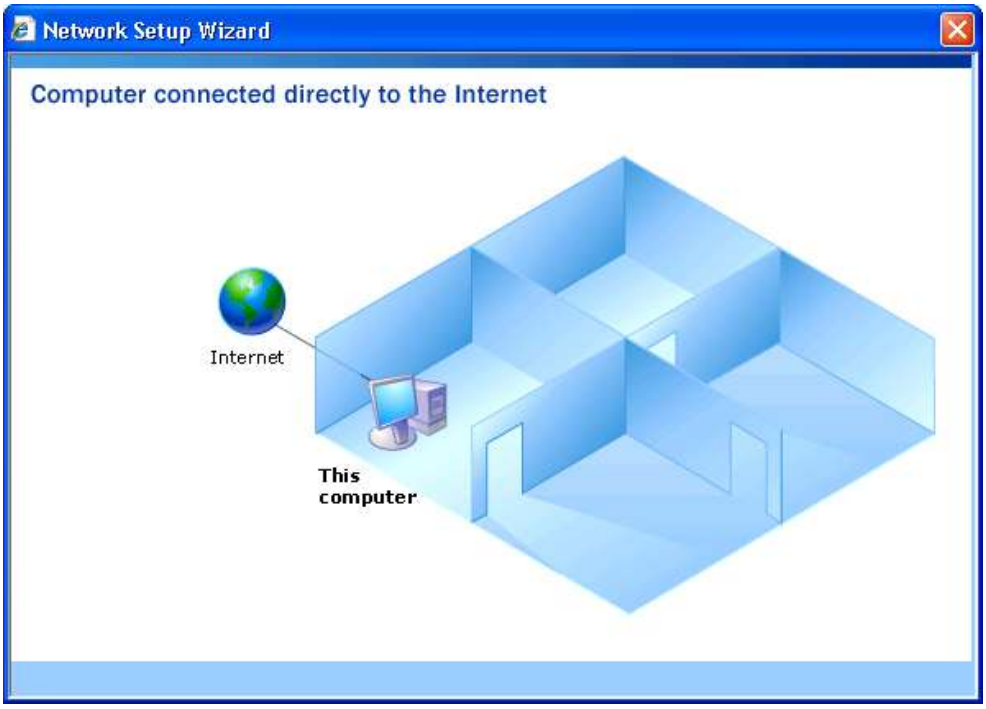
حالت سوم



کامپیوتر ها به کمک یک Hub به یکدیگر متصل شده و خود Hub نیز به اینترنت وصل است.

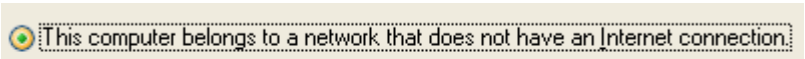
حالت چهارم

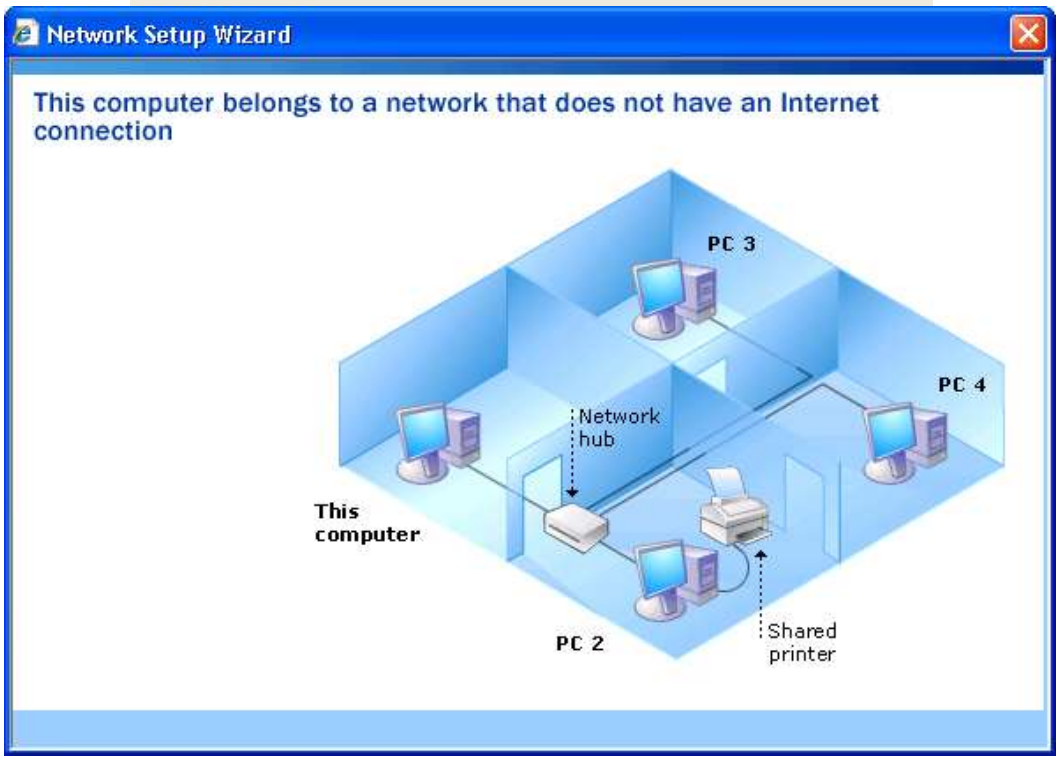




اتصال کامپیوتر خودتان به صورت مستقیم به اینترنت.

حالت پنجم

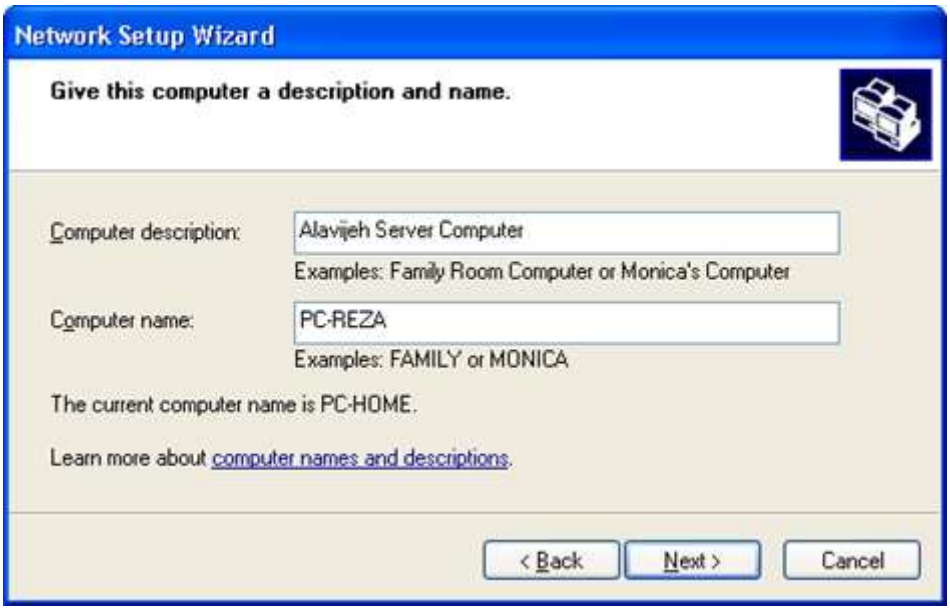




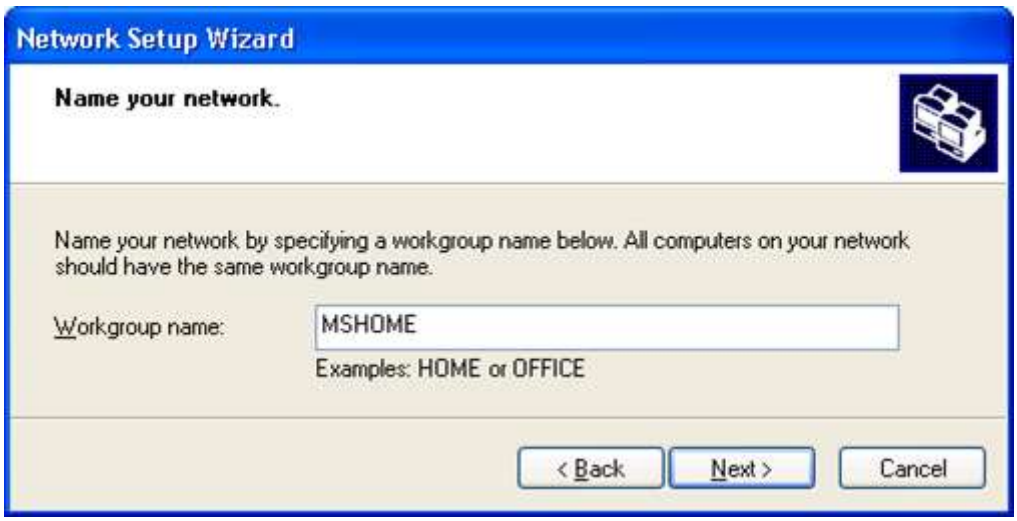
شبکه کردن کامپیوتر ها به صورت ساده.

توجه فرمایید که این حالت پنجم از همه حالت ها رایج تر است. لذا ما نیز همین حالت را انتخاب می کنیم.

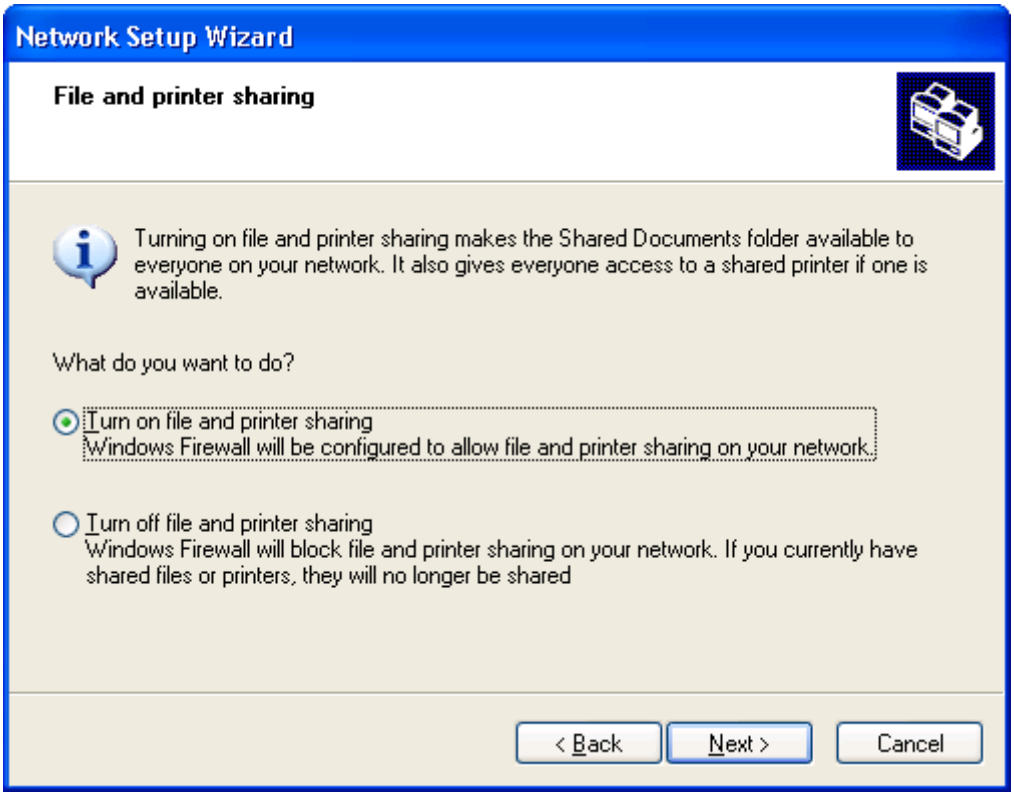
در صفحه بعدی، نام کامپیوتر در شبکه و توصیفی از آن را می نویسیم:



در صفحه بعدی، نام گروه کاری که کامپیوتر در آن قرار خواهد گرفت را وارد نمایید. گروه های کاری یک تقسیم بندی منطقی از شبکه است. مثلاً می توان یک گروه کاری برای پسران و یک گروه کاری برای دختران ایجاد نمود که **البته گروه کـاری پسران ارجحیت خواهد داشت!**

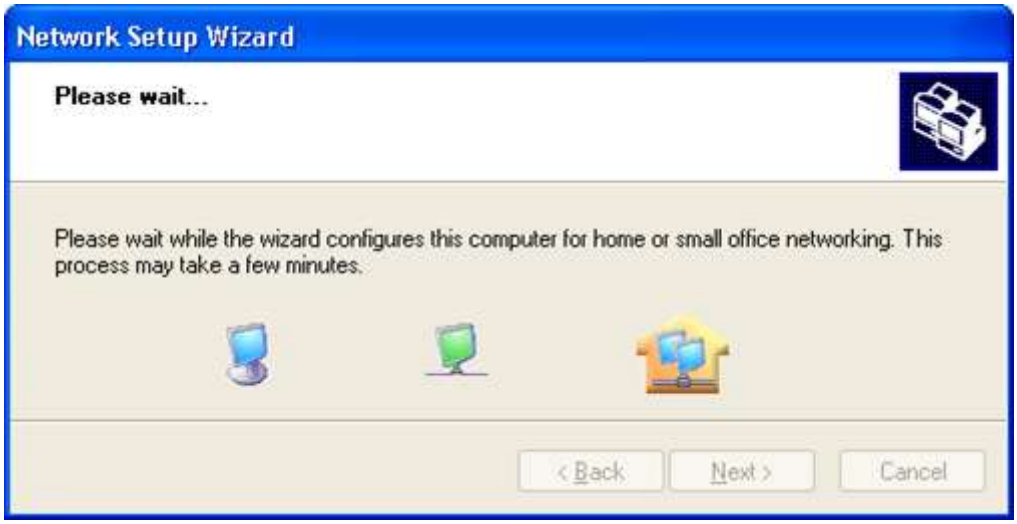


در صفحه بعد می توان تنظیم نمود که قابلیت اشتراک گذاری فایل و چاپگر فعال باشد یا نباشد که در شکل زیـر آن را فعـال کرده ایم.

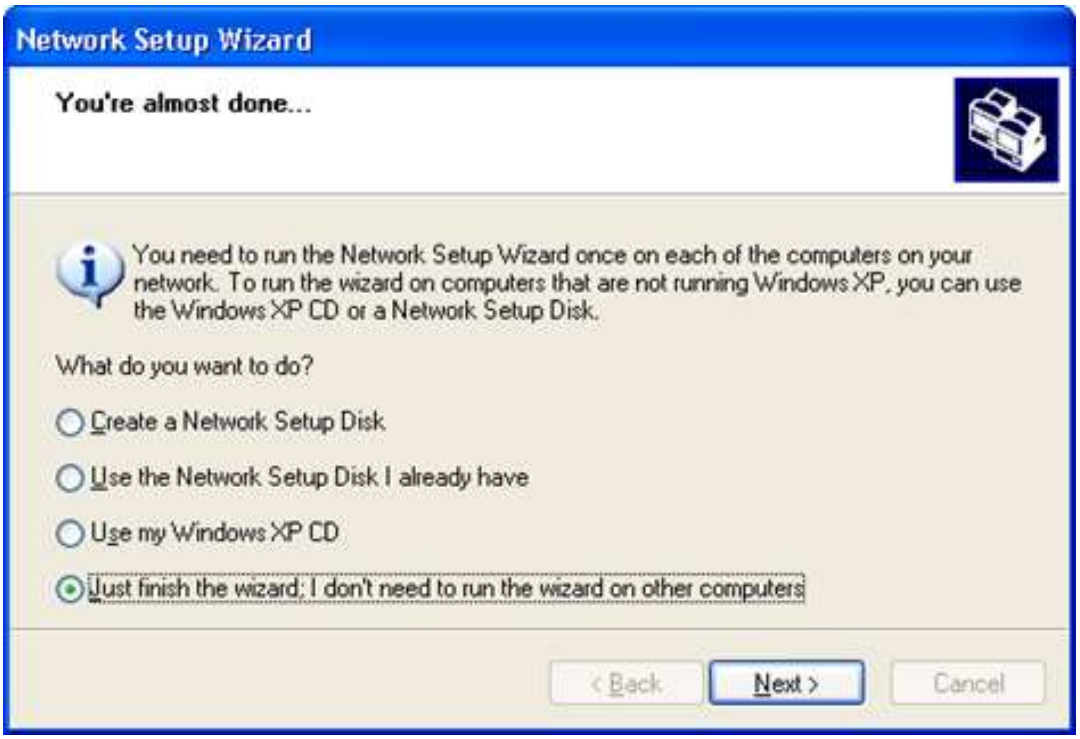


در مرحله بعد، خلاصه ای از تنظیمات انجام شده را مشاهده می کنید. برای رفتن به مرحله بعد Next بزنید:

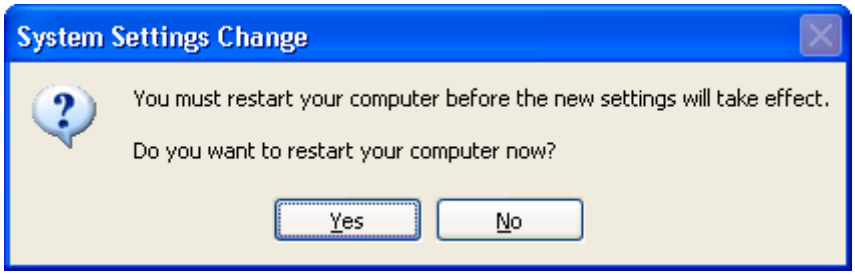
سپس سیستم شروع به راه اندازی شبکه خانگی یا محلی شما می کند.



در صفحه بعد، سیستم به شما اخطار می کند که روی دیگر کامپیوتر های موجود در شبکه نیز بایستی همین مراحل را انجام دهید؛ همچنین اخطار می دهد که اگر سیستم عامل آن ها ویندوز نباشد، به مشکل بر می خورید. گزینه آخر را انتخاب نمایید.



برای پایان نصب، Finish را بزنید. در نهایت سیستم خود را Restart نمایید.



حال در دیگر کامپیوتر ها می توانید این مراحل را انجام داده و به گروه کاری ساخته شده دسترسی پیدا کنید.

فصل ۱۱

به اشتراک گذاشتن اتصال اینترنت

۱۱-۱- مقدمه

همیشه به اشتراک گذاری اینترنت، یکی از دغدغه های راه اندازی شبکه بوده است. در گذشته نه چندان دور، سازمان های بزرگ یا اداره ها و شرکت ها، برای صرفه جویی در هزینه های اینترنت، آن را بین تمام کلاینت هایشان به اشتراک (Share) می گذاشتند. اینترنت یکی از منابعی است که می تواند در شبکه داخلی به صورت فردی یا گروهی مورد استفاده قرارگیرد لذا قابلیت به اشتراک گذاشتن این منبع بایستی وجود داشته باشد.

با گذشت زمان و با راه پیدا کردن شبکه ها به خانه های کاربران، یا به عبارتی خانگی شدن شبکه های کامپیوتری، کاربران عادی نیز به فکر اشتراک گذاری اینترنت بین سیستم های مختلف خود افتادند. اما این اقدام کمی برای یک کاربر آماتور و نا آشنا به شبکه کمی دشوار بوده و همواره نیاز بود تا متخصصان با قیمت های زیاد، آن را پیاده سازی کنند.

شرکت مایکروسافت در سیستم عامل های جدید خود امکانی را تحت عنوان ICS (Internet Connection Sharing)، به کاربران معرفی کرد تا به سادگی و بدون نیاز به هیچ دانش قبلی، و حتی متخصص این زمینه، بتوانند اینترنت خود را برای دستگاه های دیگر خود به اشتراک بگذارند.

اما همیشه سوالی بین کاربران وجود داشته که، بین چه دستگاه هایی می توان اینترنت را به اشتراک گذاشت.

به صورت کلی کامپیوتر های دسکتاپ، لبتاپ ها، Packet PC، PDA و... و هر چیزی که بتوان بر روی آن سیستم عامل نصب کنند، قادر خواهند بود از اینترنت Share شده استفاده نمایند. اما سیستم های دسکتاپ و لبتاپ بهترین گزینه به عنوان اشتراک گذارنده ها هستند. اشتراک گذاشتن آن ممکن است به وسیله ی دستگاه اکسس پوینت یا از طریق یک رایانه شخصی که مجهز به کارت شبکه باشد انجام شود. اینترنت را می توان به صورت سیمی (موسم به LAN) یا به صورت بی سیم (موسوم به WiFi) بین دو یا چند کامپیوتر به اشتراک گذاشت.

۱۱-۲- روش های به اشتراک گذاری اینترنت

اینترنت را به دو روش متداول می توان اشتراک گذاشت:

۱. وب پروکسی (Web Proxy)
۲. مترجم آدرس شبکه یا NAT

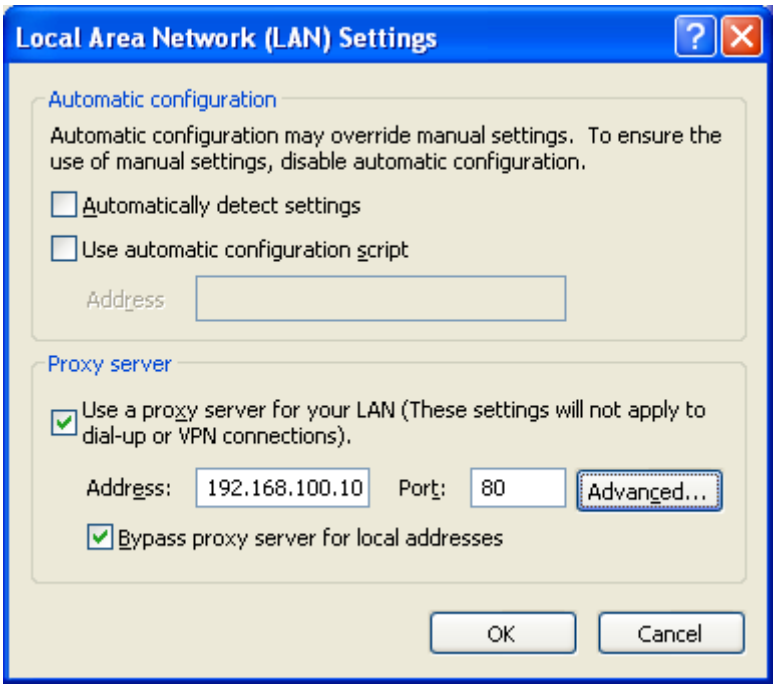
در ادامه به معرفی هر یک از روش های فوق می پردازیم.

۱۱-۳- وب پروکسی (Web Proxy)

در این روش یک نرم افزار به عنوان Proxy Server روی رایانه ای که به اینترنت متصل است، نصب می کنند و سپس سایر رایانه هایی که در شبکه می خواهند از اینترنت استفاده کنند، کلیه نرم افزار های اینترنتی مانند Internet Explorer، Messenger، Opera، DAP، IDM و ... در بخش Proxy خود بایستی آدرس **پروکسی سرور** و **پورت** را تنظیم کنند. با این کار کلیه درخواست های اینترنتی این رایانه ها از طریق آدرس و پورت تنظیم شده به رایانه اصلی (Proxy Server) و سپس از طریق آن به اینترنت ارسال شده و پاسخ آن ها نیز به همین روش دریافت می شود. ارتباط کاربران شبکه از طریق **لایه Application** انجام می شود. برای مثال، برای تنظیم Proxy Server در Internet Explorer، وارد قسمت زیر شوید:

Tools➔Internet Options ➔ Connection ➔ LAN Setting ➔ Proxy Server

حال از طریق این صفحه می توانید آدرس و پورت Proxy Server را وارد نمایید. در شکل زیر، آدرس Proxy Server برابر با ۱۹۲.۱۶۸.۱۰۰.۱۰ و شماره پورت برابر با ۸۰ می باشد.



۱۱-۳-۱- مزایای روش وب پروکسی

الف) اعتبار سنجی (Authentication): اعتبار سنجی به این معنی است که می توان برای کاربرانی که می خواهند از اینترنت در شبکه استفاده کنند، نام کاربری و کلمه عبور تعریف کرد و میزان دسترسی آن ها به اینترنت را محدود کرد.

ب) ثبت عملکرد کاربر (User Log): با این امکان می توان از کارکرد کاربران شبکه گزارش تهیه کرد. این گزارش شامل سایت هایی که کاربر دیده است، نوع استفاده از اینترنت از لحاظ سرویس های شبکه مانند FTP، Http، Chat و ... و نیز حجم یا ترافیک استفاده از شبکه برای دانلود یا آپلود اطلاعات می باشد.

ج) دیوار آتشین شخصی (Personal Firewall): از طریق این گزینه می توان از نفوذ و دسترسی کاربران سایر شبکه ها به شبکه داخلی جلوگیری کرد و همچنین می توان سرویس های شبکه یا اسامی و سایت های اینترنتی خاصی را مسدود یا Block نمود.

د) نگهداری اطلاعات وب (Web Caching): کلیه سایت ها و اطلاعاتی که کاربران از شبکه دریافت می کنند، در بخشی از دیسک کپی شده و درخواست های بعدی کاربران شبکه، با این اطلاعات مقایسه می شوند. اگر درخواست ها در دیسک سخت وجود داشته باشند، به سمت کاربر ارسال می شوند و در غیر این صورت، درخواست مذکور به سمت اینترنت ارسال شده و نتایج حاصل به سمت کاربر ارسال می شود. به این عملیات Web Caching می گویند و برای بالا بردن سرعت استفاده از اینترنت و کاهش ترافیک شبکه مورد استفاده قرار می گیرد.

۱۱-۳-۲- معایب وب پروکسی

الف) زمان بر بودن تنظیم: برای اتصال به شبکه باید در همه رایانه ها تنظیمات خاصی را در بخش Proxy ویندوز انجام داد و در شبکه های بزرگ، انجام این کار وقت زیادی را می گیرد. البته برای تنظیم Proxy در Internet Explorer، می توان با کمک Group Policy، این تنظیم را روی تمامی سیستم ها اعمال نمود. بدین منظور به فصل Group Policy مراجعه فرمایید.

ب) عدم شفافیت: نوع ارتباط، شبکه شفاف (Transparent Network) نیست؛ به این معنی که کاربران شبکه اطلاع دارند که از سمت سرویس دهنده به طور کامل کنترل می شوند.

ج) وابستگی به پروکسی سرور: در صورتی که نرم افزار پروکسی دچار مشکل شود، اینترنت تمامی کاربران قطع می شود. از نرم افزار های رایج به عنوان Proxy Server می توان به ISA Server، Win Route و CCProxy Server اشاره کرد.

۱۱-۴- مترجم آدرس شبکه یا NAT

در روش مترجم آدرس شبکه یا NAT (Network Address Translator) دیگر نیازی به نصب برنامه خاصی در ویندوز نیست، بلکه با استفاده از سرویس ویندوز ICS (Internet Connection Sharing) می توان اینترنت را برای کاربران در شبکه به اشتراک گذاشت. تنها نکته مهم برای برقراری ارتباط بین شبکه و سرور این است که بایستی آدرس Gateway تمامی رایانه های شبکه با آدرس رایانه سرور یکی باشد و در بخش DNS رایانه های شبکه، بایستی آدرس DNS Server را وارد نماییم تا عملیات تبدیل نام در شبکه انجام شود.

۱۱-۴-۱- مزایا و معایب روش NAT

الف) نوع ارتباط شبکه شفاف است؛ به این معنی که کاربران از نوع سرویس دهنده اینترنت هیچ اطلاعی ندارند.

ب) رایانه های داخل شبکه نیاز به تنظیمات Proxy ندارند.

ج) در این روش، چون ارتباط کاربران در **لایه Network** انجام می شود، عملیات اعتبار سنجی، صبت عملکرد کاربر، دیوار آتشین شخصی و نگهداری اطلاعات وب (Web Caching) را نمی توان انجام داد.

نکته: نرم افزار Microsoft ISA Server یکی از قوی ترین برنامه های به اشتراک گذاری اینترنت است که می تواند با هر دو روش فوق اینترنت را برای کاربران داخل شبکه به اشتراک بگذارد. این نرم افزار از یک دیوار آتشین (Firewall) بسیار قوی برای حفاظت رایانه های داخل شبکه استفاده می کند و می تواند تمامی کاربران داخل شبکه را بسیار قوی مدیریت کند. از دیگر ویژگی های مهم این نرم افزار، Cache Server قدرتمند آن می باشد.

۱۱-۵- آموزش عملی وب پروکسی یا Proxy Server

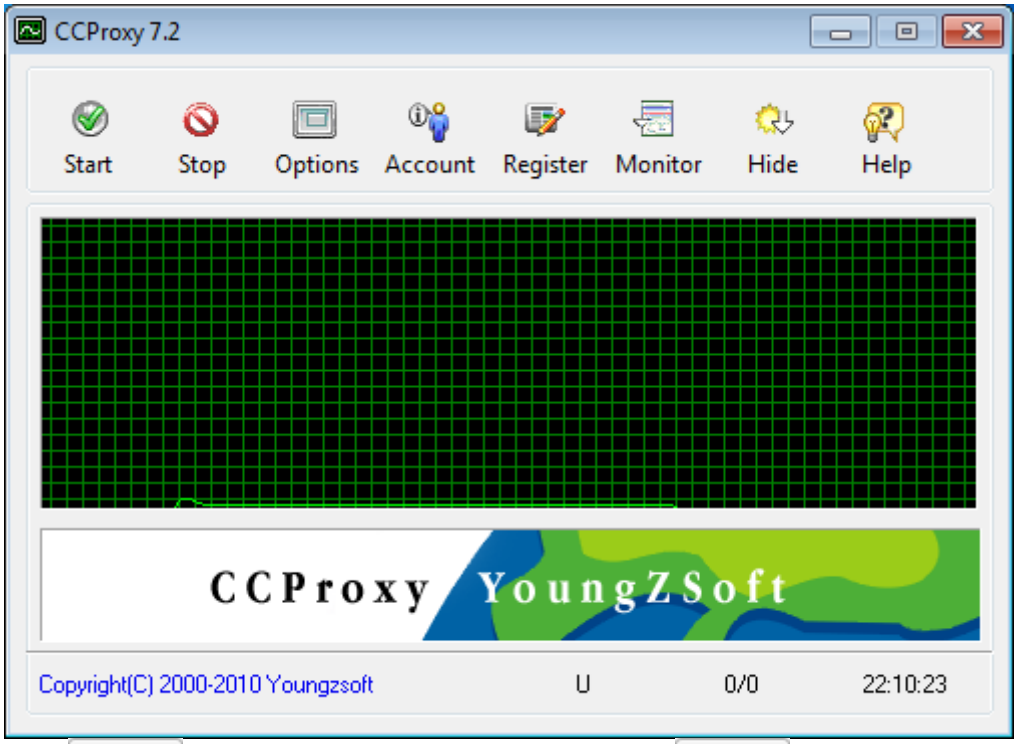
گفتیم که یکی از روش های به اشتراک گذاری اینترنت، استفاده از وب پروکسی یا Proxy Server می باشد. در این قسمت، ما به آموزش یک نرم افزار Proxy Server به نام **CCProxy** می پردازیم. جهت استفاده از این نرم افزار، پس از نصب آن، حتما

اقدام به ثبت آن نمایید زیرا نسخه ثبت نشده، تنها قادر به سرویس دهی به ۳ کاربر به صورت همزمان می باشد؛ اما نسخه ثبت شده هیچ محدودیتی در سرویس دهی ندارد. این نرم افزار بسیار کم حجم بوده (حدود MB۲) و امکان دانلود آن از اینترنت وجود دارد.

۱۱-۵-۱- تنظیمات سرور

پس از نصب نرم افزار CCProxy روی کامپیوتری که به اینترنت وصل است (کامپیوتر سرور) و باز کردن آن، صفحه ای مانند زیر مشاهده می نمایید. کاربرد دکمه های اصلی نرم افزار به صورت زیر می باشد:

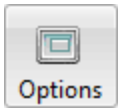
- Start: با کلیک روی این دکمه، نرم افزار شروع به سرویس دهی می کند و کلاینت ها می توانند از اینترنت آن استفاده نمایند.
- Stop: با کلیک روی این دکمه، نرم افزار عمل سرویس دهی را قطع می کند.
- Options: از طریق این قسمت می توان تنظیمات عمومی نرم افزار، مانند پورت های مورد استفاده را تغییر داد.
- Account: از طریق این قسمت می توان حساب های کاربران را مدیریت نمود.
- Register: از طریق این قسمت می توان اقدام به ثبت نرم افزار و حذف محدودیت های آن نمود.
- Monitor: از طریق این قسمت می توان عملیات آمار گیری را انجام داد.
- Hide: با کلیک روی این دکمه، صفحه اصلی نرم افزار مخفی شده و آیکون نرم افزار در System Tray باقی مانده و نرم افزار به سرویس دهی خود ادامه می دهد.
- Help: با کلیک روی این دکمه، یک فایل PDF باز می شود که در اصل همان Help نرم افزار می باشد.
- نکته: اگر برنامه را ببندید، سرویس دهی نرم افزار قطع می شود و دیگر کلاینت ها قادر به گرفتن اینترنت از سرور نیستند. جهت مخفی کردن نرم افزار، روی دکمه Hide کلیک کنید.



برای شروع سرویس دهی، روی دکمه 

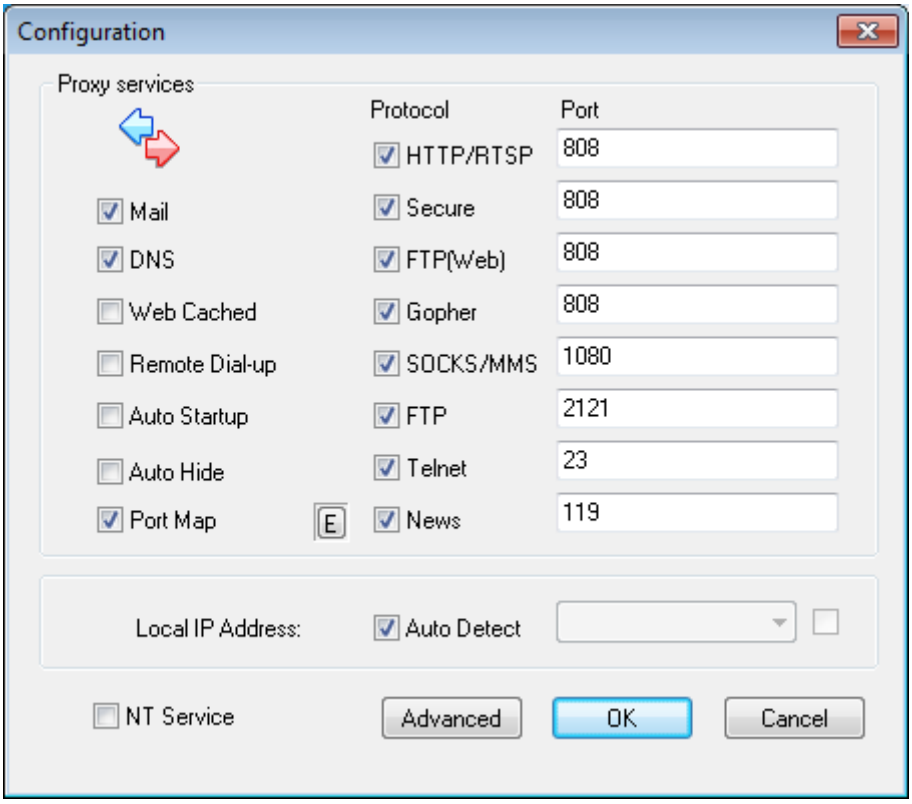
و برای قطع عمل سرویس دهی روی دکمه 

کلیک نمایید.

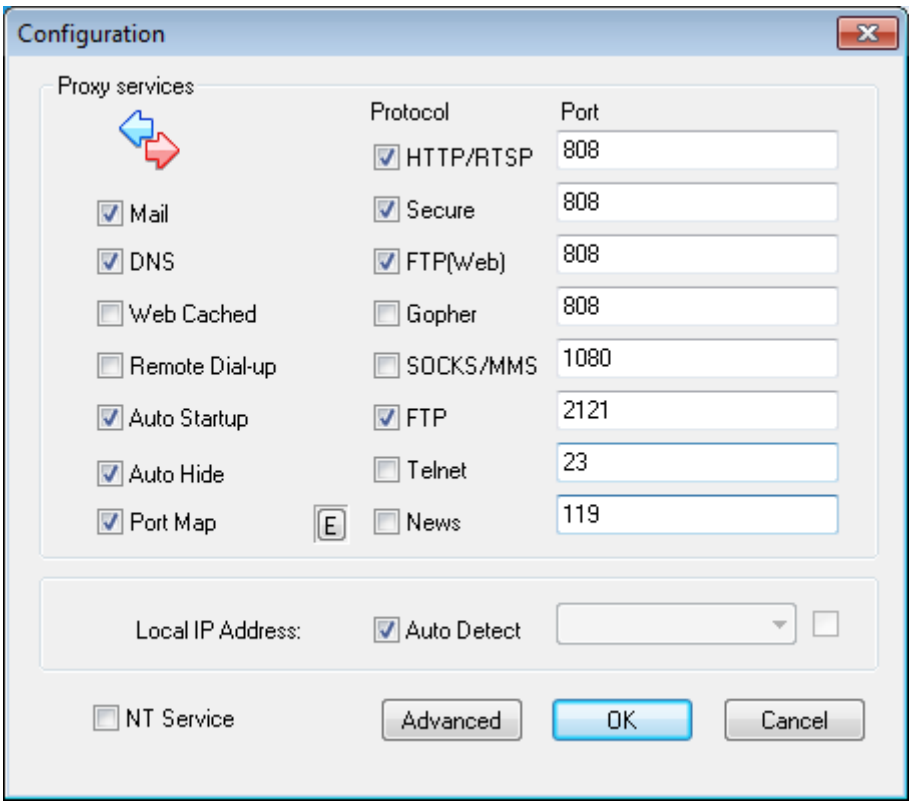
حال نوبت به تنظیمات عمومی برنامه می رسد. بدین منظور روی دکمه 

کلیک نمایید.

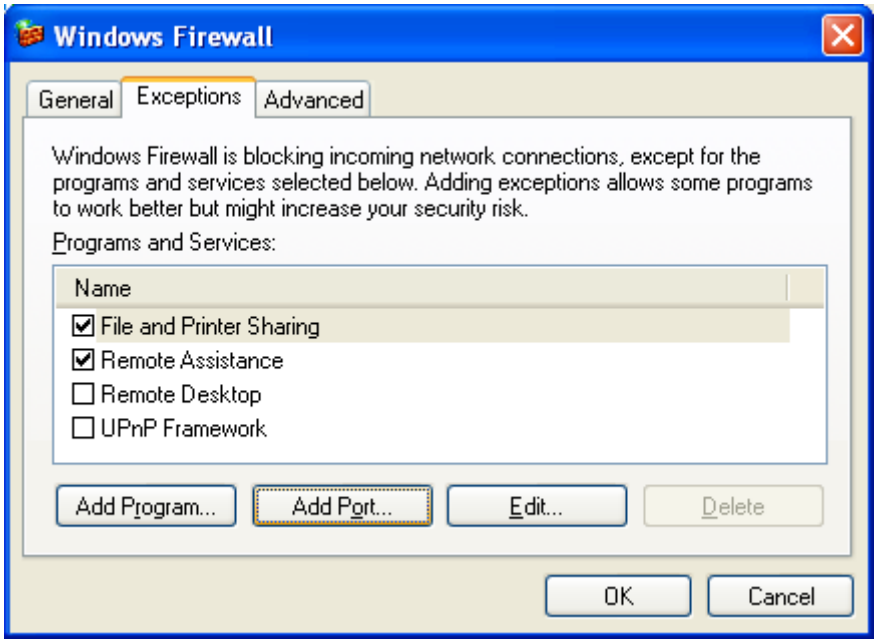
در صفحه باز شده، می توانید تنظیمات عمومی برنامه را مشاهده نمایید. اصلی ترین تنظیمات شامل سرویس های قابل ارائه توسط نرم افزار و شماره پورتی که هر سرویس اشغال می کند می باشد.



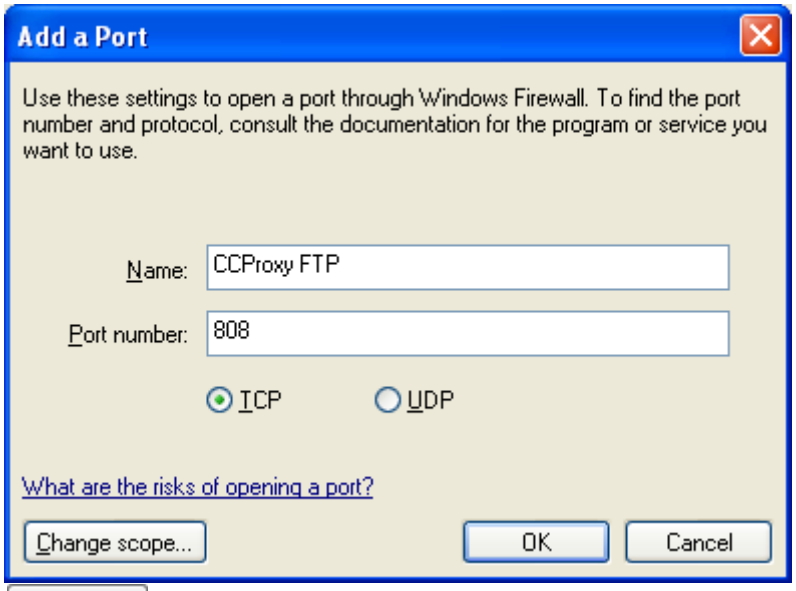
همانطور که در شکل فوق مشاهده نمودید، به صورت پیش فرض تمامی سرویس های قابل ارائه فعال می باشند، این امر هم باعث افت کارآیی نرم افزار می شود و هم باعث می شود برخی پورت ها بی دلیل اشغال شوند. به همین دلیل توصیه می شود سرویس هایی که به آن نیاز ندارید را غیر فعال نمایید. مثلاً سرویس Gopher یک سرویس قدیمی است که پروتکل Http جایگزین آن شده است. در صورت نیاز می توانید شماره پورت را نیز تغییر دهید؛ فقط توجه نمایید که شماره پورت های وارد شده نباید با شماره پورت دیگر نرم افزار ها تداخل داشته باشد. ما سرویس های خود را به صورت زیر فعال نمودیم:



در صورتی که Firewall کامپیوتر شما فعال باشد، بایستی این شماره پورت ها (تصویر فوق) را به Firewall معرفی نمایید. بدین منظور ابتدا Firewall را از Control Panel باز نموده و سپس وارد سربرگ Exceptions شوید.

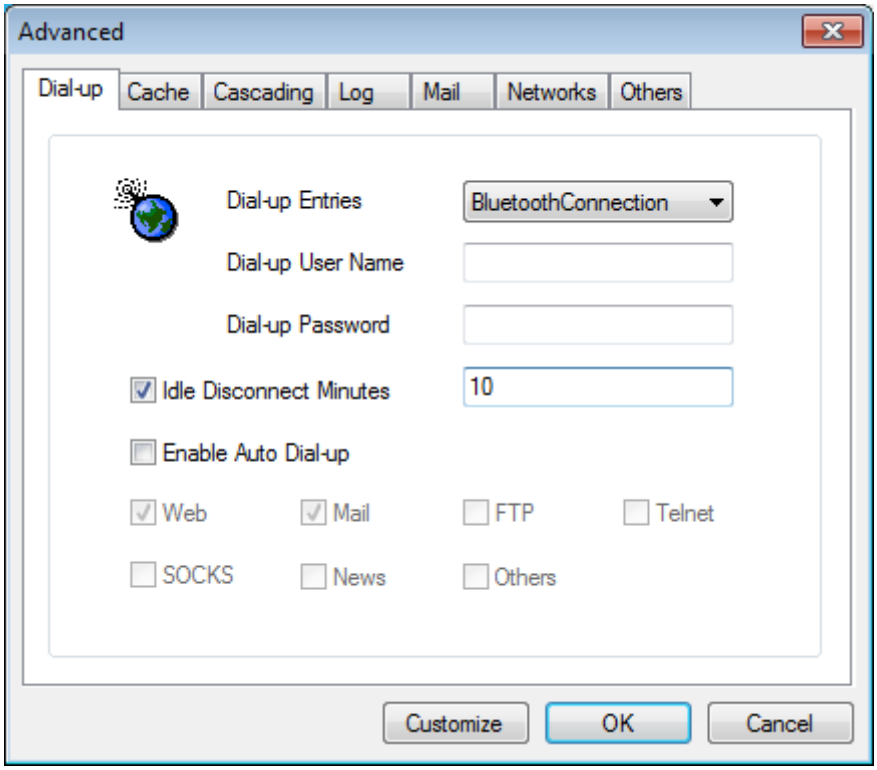


سپس روی دکمه Add Port کلیک نموده و سپس شماره پورت مورد نظر به همراه یک نام دلخواه برای آن وارد نمایید. به ازاء پورت های با شماره مختلف، این کار را چندین بار تکرار نمایید.

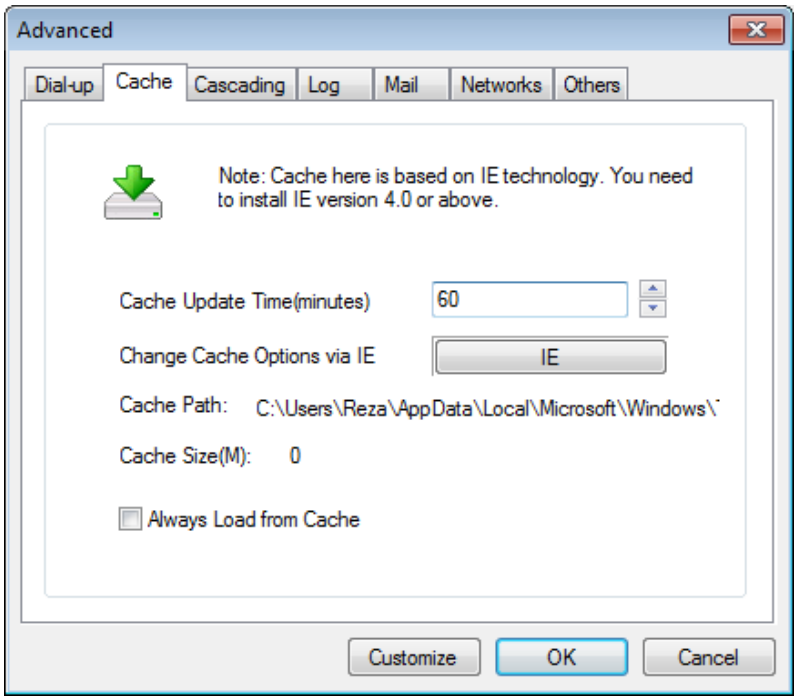


صفحه Options دارای تنظیمات پیشرفته تری نیز می باشد. بدین منظور روی دکمه Advanced کلیک نمایید. در صفحه باز شده، تعدادی سربرگ وجود دارد که آن ها را مختصرا توضیح می دهیم:

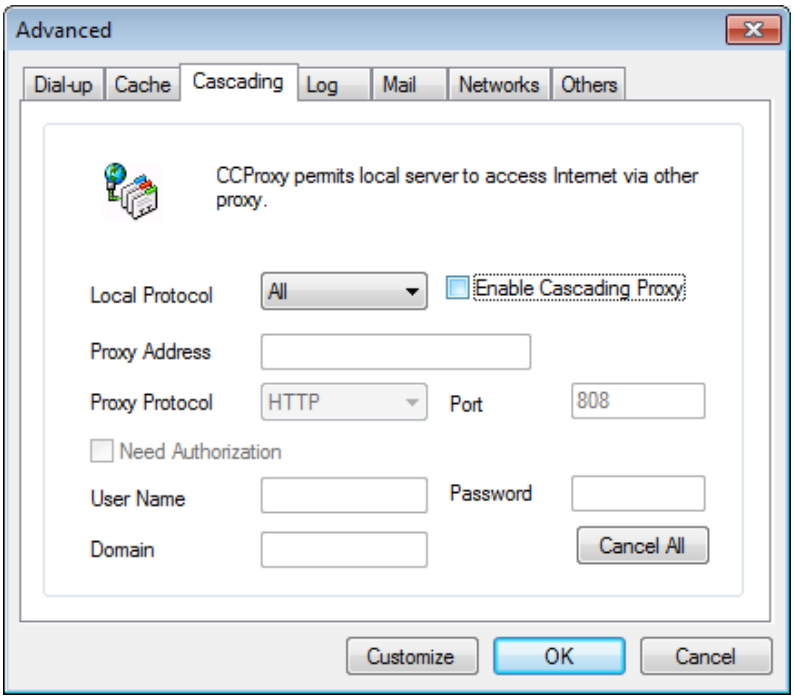
Dial-UP: در این سربرگ می توان مشخص نمود که از کدام Connection و با چه Username و Passwordی به اینترنت وصل شوید (خود سرور به اینترنت وصل شود و نه کلاینت ها). همچنین می توان مشخص نمود که اگر تا چند دقیقه هیچ درخواستی به Proxy Server ارسال نشد، اتصال سرور با اینترنت قطع شود (در این مثال ۱۰ دقیقه). امکان دیگری که این صفحه دارد، این است که می توان مشخص نمود که اگر درخواست های خاصی مانند Web، Email، FTP یا ... به سمت سرور آمد و سرور به اینترنت متصل نبود، عمل اتصال به اینترنت و انجام عمل سرویس دهی به صورت خودکار انجام گیرد.



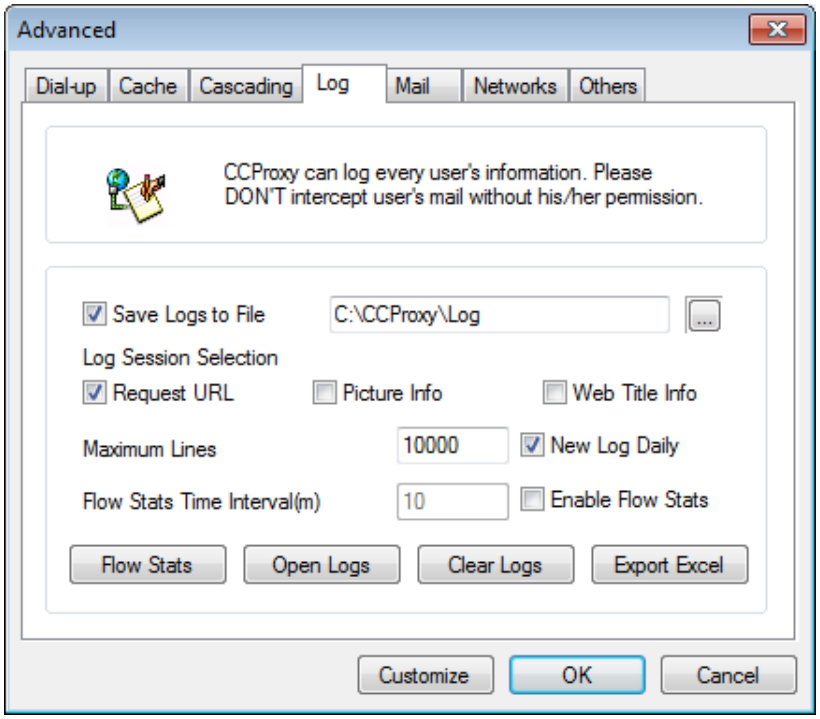
Cache: همانطوری که قبلاً توضیح دادیم، یکی از مزایای Web Proxyها، ذخیره صفحات وب یا اصطلاحا Caching می باشد. در این سربرگ شما می توانید تنظیمات Caching را تغییر دهید. مثلاً در شکل زیر مشخص شده است که با باز شدن هر صفحه وب، اطلاعات آن صفحه به مدت ۶۰ دقیقه ذخیره شود و در درخواست های بعدی، در صورت امکان از این صفحات ذخیره شده استفاده نماید. مسیر ذخیره فایل های Cache شده نیز مشخص است. برای انجام تنظیمات بیشتر، روی دکمه IE کلیک نمایید.



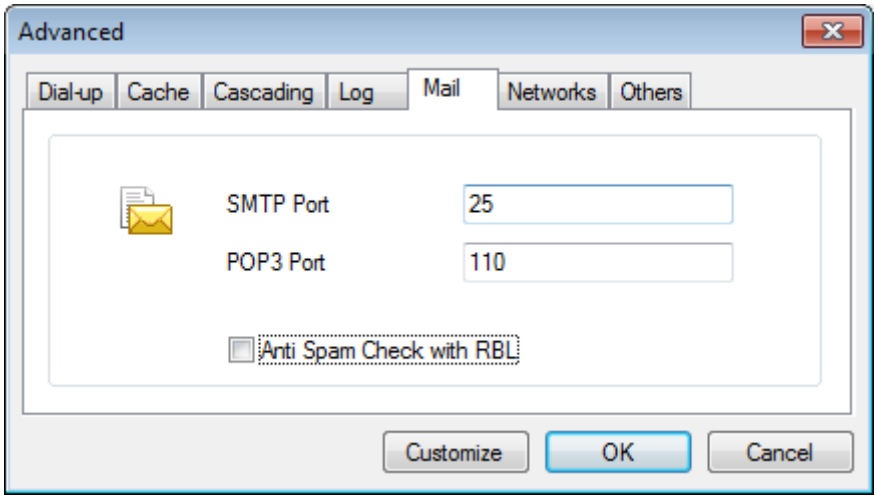
Cascading: این سربرگ زمانی استفاده می شود که خود Proxy Server ما، اینترنت را از یک Proxy Server دیگر دریافت نماید. در اینجا می توان تنظیمات مورد نیاز مانند آدرس و شماره پورت Proxy Server، نام کاربری، رمز عبور و ... را تعیین نمود.



Log: همانطور که قبلاً نیز بحث شد، یکی از مزایای Web Proxy، امکان رد گیری اتفاقات انجام شده، مثلاً تلاش های کاربران برای مشاهده سایت های مختلف یا میزان داده های مورد استفاده هر کاربر می باشد. این اطلاعات در فایل هایی به نام Log File ذخیره می شود. از طریق این صفحه می توانید تنظیمات Log File ها را انجام دهید. ساختار Log File ها بدین صورت است که نرم افزار به ازاء هر روز، دو فایل متنی می سازد، یکی برای سایت مورد دسترسی قرار گرفته (LogYYYYMMDD.txt) و دیگری برای میزان داده ارسالی و دریافتی هر کاربر (DataYYYYMMDD.txt). در این صفحه با کلیک روی دکمه Open Logs می توانید محتوای Log File را با Note Pad مشاهده نمایید. با کلیک روی دکمه Export Excel نیز می توانید Log File را به یک فایل Excel تبدیل نموده و داده ها را ساخت یافته مشاهده نمایید.

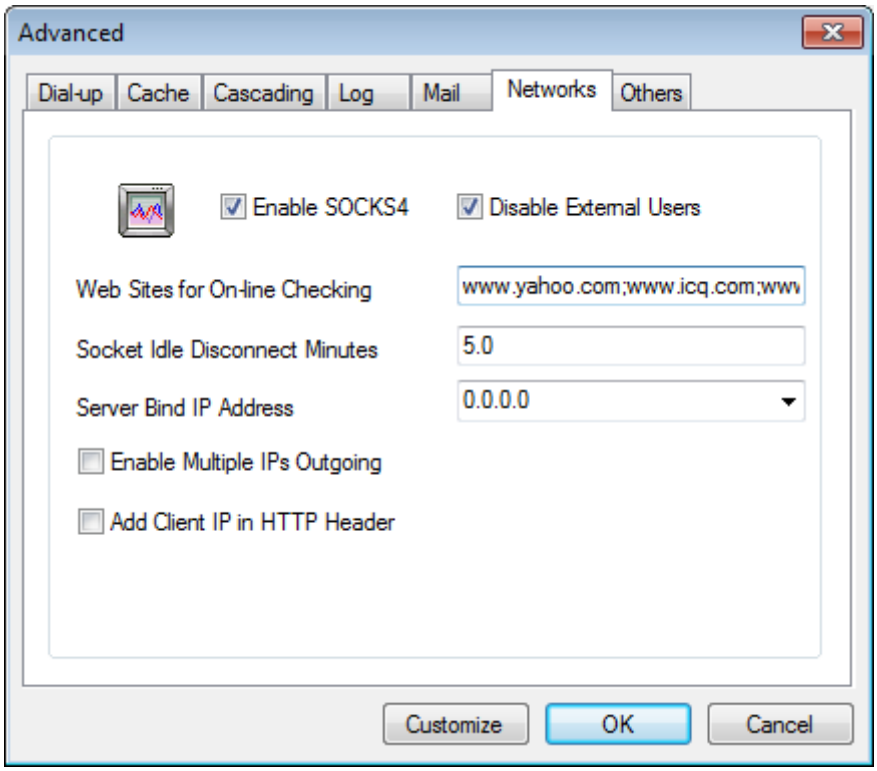


Mail: از طریق این سربرگ می توانید مشخص نمایید که سرویس های ایمیل SMTP و POP3 از طریق کدام پورت ها کار بکنند. این پارامتر ها بیشتر هنگام کار با نرم افزار های مدیریت ایمیل مانند Outlook Express نمود پیدا می کنند. امکان بررسی وجود Spam در ایمیل ها نیز وجود دارد.

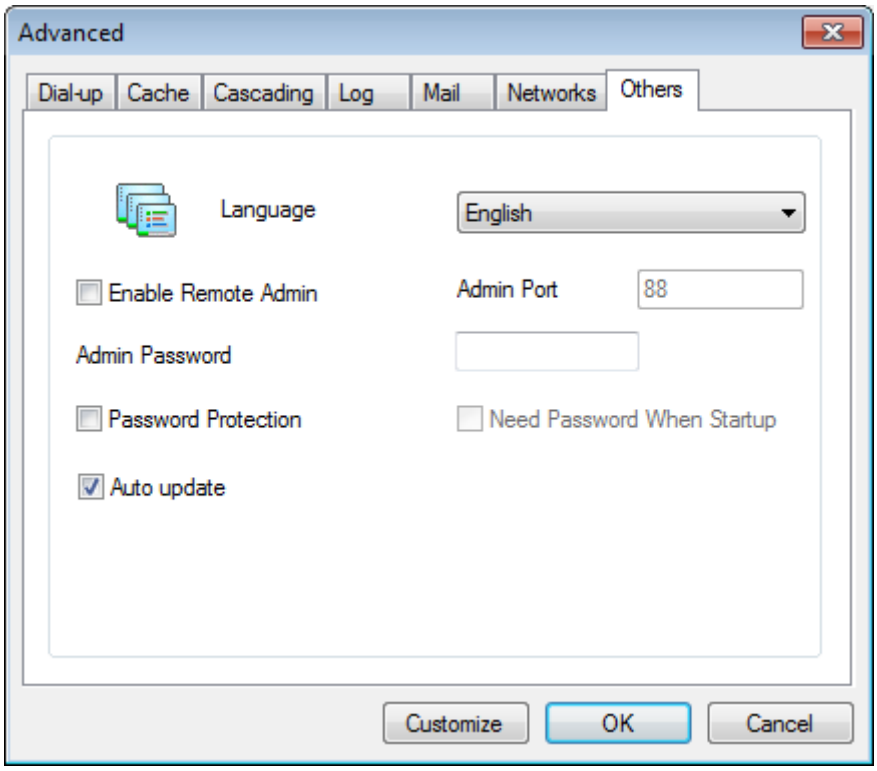


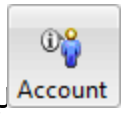
Networks: این سربرگ نیز تنظیمات خاصی را انجام می دهد که هر کدام را به اختصار توضیح می دهیم:

- Enable SOCKS4: فعال سازی سرویس های SOCKS4 و SOCKS4A که در Web Proxy ها کاربرد دارد.
- Enable External Users: فعال کردن یا غیر فعال کردن دسترسی کاربران خارج از شبکه LAN.
- Web Sites For On-Line Checking: این نرم افزار نیاز دارد بداند که آیا سیستم سرور به اینترنت متصل است یا خیر؟ که بدین منظور بایستی سایت های خاصی را ملاقات نماید. در این قیمت می توانید سایت های خاصی را مشخص نمایید که در صورتی هیچ کدام از آن ها باز نشود، یعنی اینترنت ما قطع شده است.
- Socket Idle Disconnect Minutes: مدت زمان Time Out سوکت های بدون استفاده.
- Server Bind IP Address: زمانی که کامپیوتر سرور دارای چندین آدرس IP باشد (Multiple Host)، می توان آدرس IP خاصی را برای نرم افزار تعیین نمود. آدرس ۰.۰.۰.۰ بدین معناست که نرم افزار خودش یک آدرس IP را خودکار انتخاب نماید.
- Enable Multiple IPs Outgoing: اگر چندین آدرس IP دارید و می خواهید کاربران هنگام اتصال به اینترنت، هر کدام یک آدرس IP جدا داشته باشند، این گزینه را فعال نمایید.
- Add Client IP in HTTP Header: نرم افزار به سرآیند HTTP، "X-Forwarded-For" را اضافه می کند که "X-Forwarded-For" شامل آدرس IP کلاینت خواهد بود.

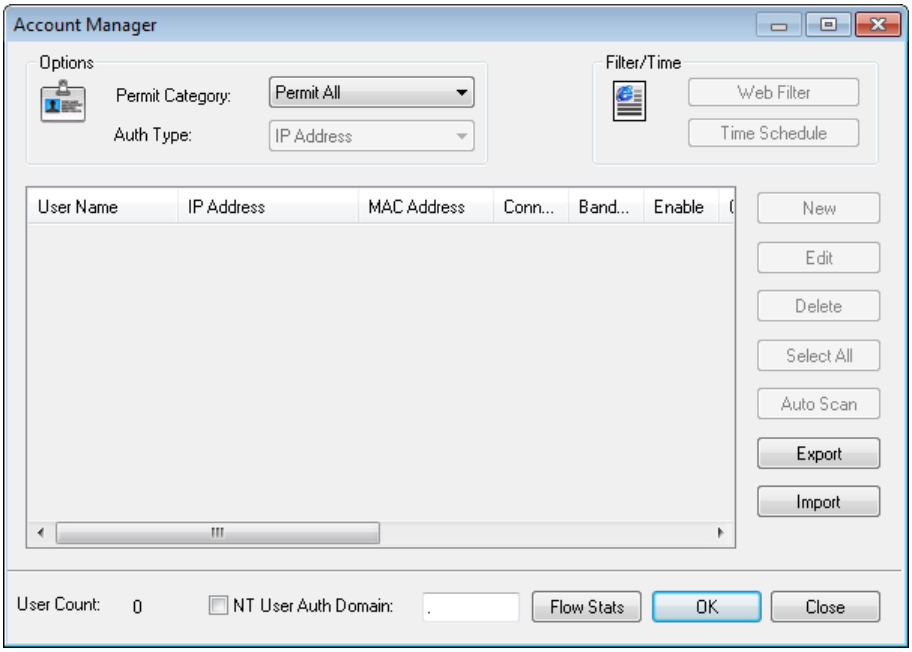


Others: از طریق این سربرگ می توان تنظیمات عمومی دیگری انجام داد، مانند زبان نرم افزار، رمز عبور مـدیر (Admin)، امکان به روز رسانی خودکار و ....

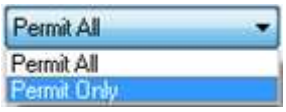


حال نوبت به تنظیمات حساب های کاربری می رسد. اگر تنظیمات این قسمت را وارد ننمایید، هر کـامپیوتری کـه بـه شـبکه متصل باشد، می تواند از اینترنت به اشتراک گذاشته شده استفاده نماید. اگر این امر مورد پسند شما نیسـت و دوسـت داریـد کاربران را کنترل نمایید، در صفحه اصلی نرم افـزار، روی دکمـه 

لیـک کنیـد. در صـفحه بـاز شـده امکـان انجـام تنظیمات حساب های کاربری وجود دارد که آن ها را در ادامه توضیح می دهیم.



در ابتدای امر و در قسمت Permit Category مشخص می شود که اجازه های دسترسی جهت استفاده از اینترنت به اشتراک گذاشته شده چگونه باشد. در ابتدا گزینه Permit All انتخاب شده است، یعنی تمامی کاربران شبکه LAN حق استفاده از این اینترنت را دارند. اما اگر می خواهید دسترسی ها به اینترنت را تحت کنترل خود در آورید، گزینه دوم یعنی Permit Only را انتخاب نمایید.

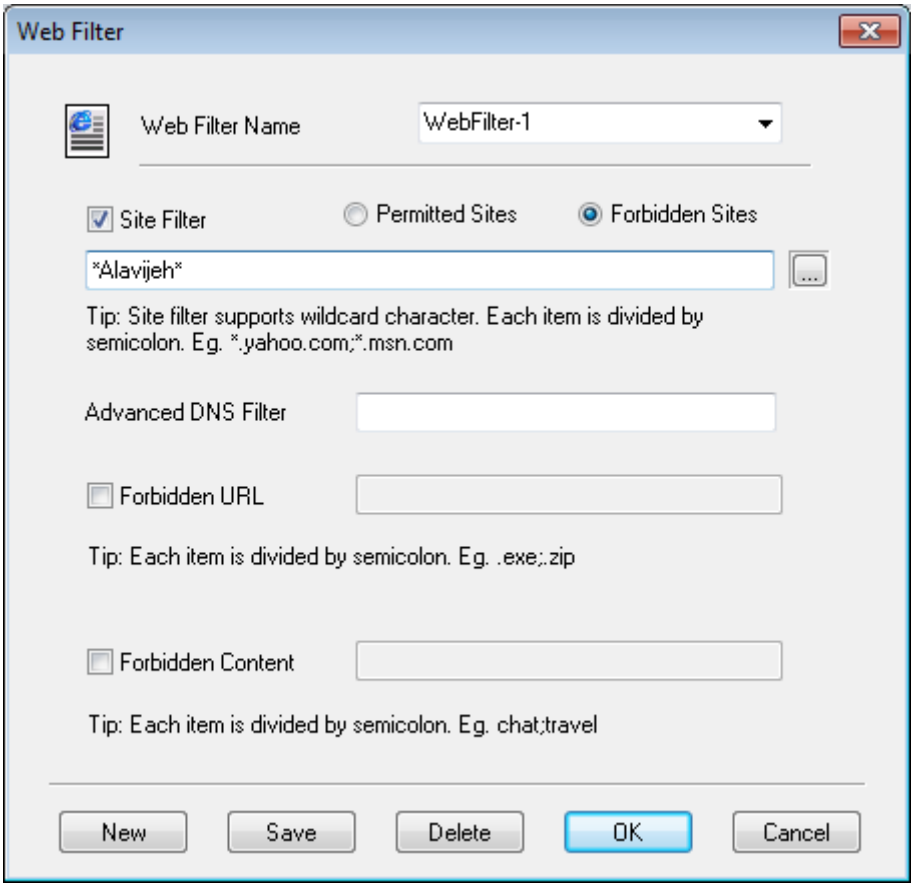


با انتخاب این گزینه، دکمه های این صفحه فعال شده و امکان مدیریت حساب های کاربری فراهم می شود. سپس بایستی نوع احراز هویت و اجازه دسترسی با اینترنت را مشخص نمایید. این کار از طریق قسمت Auth Type انجام می گیرد. معنای گزینه های این قسمت به صورت زیر است:

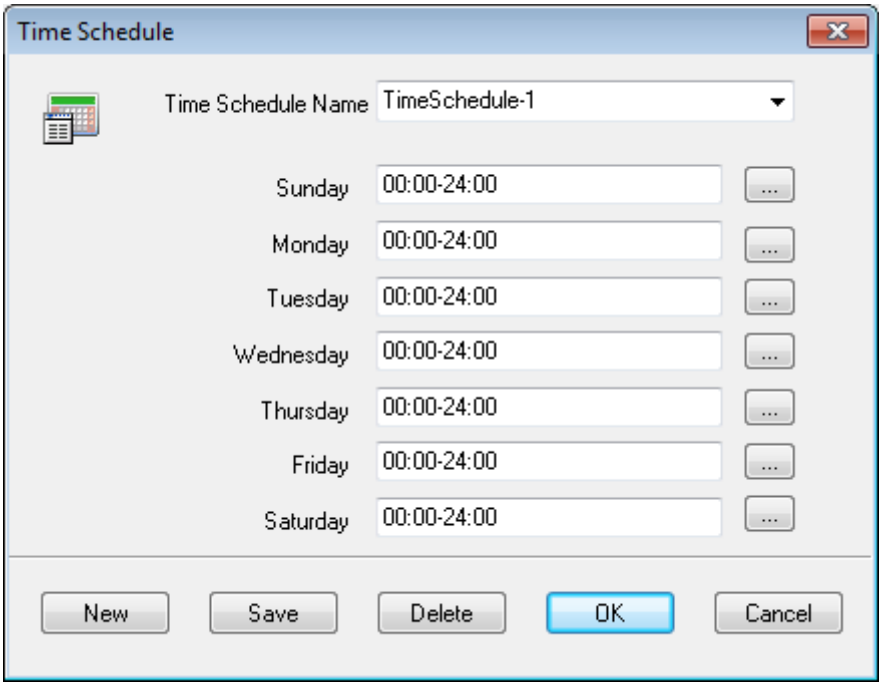
- **IP Address**: فقط کاربرانی حق استفاده از اینترنت را دارند که آدرس IP سیستم آن ها در لیست زیر ثبت شده باشد.
- **MAC Address**: فقط کاربرانی حق استفاده از اینترنت را دارند که آدرس MAC کارت شبکه آن ها در لیست زیر ثبت شده باشد.
- **User/Password**: فقط کاربرانی حق استفاده از اینترنت را دارند که نام کاربری و رمز عبور آن ها در لیست زیر ثبت شده باشد. این کاربران هنگام استفاده از اینترنت، بایستی نام کاربری و رمز عبور را وارد نمایند و اگر نام کاربری و رمز عبور وارد شده در لیست زیر موجود باشد، آن ها اجازه استفاده از اینترنت را پیدا می کنند.
- **User/Password + IP**: فقط کاربرانی حق استفاده از اینترنت را دارند که نام کاربری و رمز عبور آن ها به همراه آدرس IP سیستم آن ها در لیست زیر ثبت شده باشد. با این کار، تقریباً می توان گفت که کاربران را مجبور به استفاده از سیستمی خاص می کنیم، اما این امر همیشه صحیح نیست، زیرا آدرس IP کامپیوتر ها قابل تغییر است.
- **User/Password + MAC**: فقط کاربرانی حق استفاده از اینترنت را دارند که نام کاربری و رمز عبور آن ها به همراه آدرس MAC کارت شبکه آن ها در لیست زیر ثبت شده باشد. با این کار، کاربران را مجبور به استفاده از سیستمی خاص می کنیم.

- **IP + MAC:** فقط کاربرانی حق استفاده از اینترنت را دارند که آدرس IP سیستم آن ها به همراه آدرس MAC کارت شبکه آن ها در لیست زیر ثبت شده باشد. با این کار سیستم ها را مجبور می کنیم کـه هـر سیسـتم، یـک آدرس IP خاص داشته باشد که در صورت تغییر آدرس IP دیگر امکان اتصال به اینترنت وجود نداشته باشد.

یکی دیگر از امکانات این نرم افزار، فیلتر کردن سـایت هـای مـورد دسترسـی کـاربران مـی باشـد. بـدین منظـور روی دکمـه Web Filter کلیک نمایید. در این صفحه می توانید مشخص نمایید که فقط سایت هایی با ویژگی های زیر قابـل بـاز شدن باشد (Permitted Sites) یا فقط سایت هایی با ویژگی های زیر مسدود و قدغن باشد (Forbidden Sites) که البته مورد دومی پر کاربرد تر است. سپس در جعبه متن Site Filter، آدرس سایت های مورد نظر را وارد نمایید. بـرای اسـتفاده از کلـی گویی می توان از علامت * (به معنای صفر یا چند حرف) استفاده کرد. در قسمت Forbidden URL مـی تـوان برخـی URL های ممنوعه را وارد نمود. مثلاً URL هایی که در آن ها حروف .exe یا .zip وجود دارد. این بخش بیشـتر بـرای جلـوگیری از عملیات دانلود می باشد. در قسمت Forbidden Content نیز می توان مشخص نمود که اگر یک صفحه درخواستی شامل متن و محتوای خاصی بود، آن را به سمت کاربر ارسال نکن. می توان چندین نوع فیلتر را تعریف نمـود و هـر کـدام را بـه کـاربری خاص نسبت داد. این کار در هنگام ایجاد کاربر جدید انجام می گیرد.



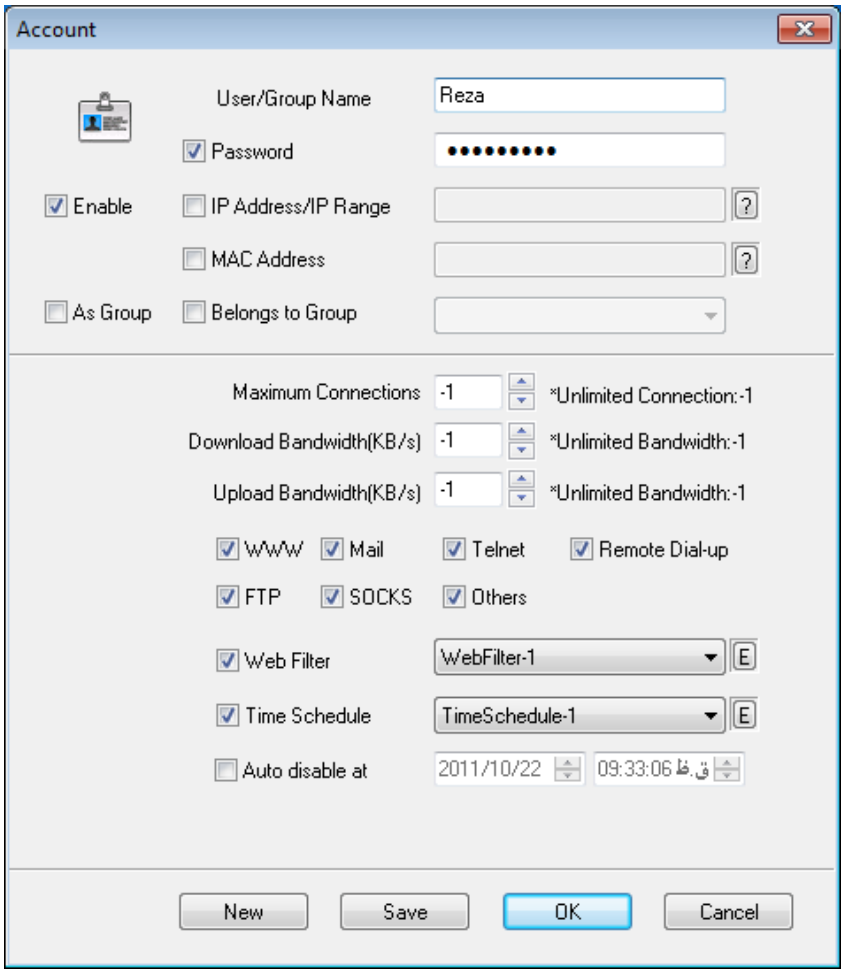
یکی دیگر از امکانات این نرم افزار، امکان زمانبندی سرویس دهی نرم افزار می باشد. بدین منظـور در صـفحه Accounts روی دکمه Time Schedule کلیک کنید. در صفحه باز شده می توانید مشخص نمایید که نرم افزار در چـه روز هـایی و از چـه ساعت تا چه ساعت هایی، عمل سرویس دهی را انجام دهد. می توان چندین نوع زمان بندی را تعریف نمود و هر کـدام را بـه کاربری خاص نسبت داد. این کار در هنگام ایجاد کاربر جدید انجام می گیرد.



حال نوبت به یکی از مهم ترین بخش های نرم افزار یعنی حساب های کاری کاربران می رسد. برای ایجاد حساب کاربری جدید، در صفحه Accounts روی دکمه New کلیک کنید. برای تغییر اطلاعات کاربران موجود نیز، پس از انتخاب کاربری خاص روی دکمه Edit کلیک نمایید. حذف کاربر نیز با دکمه Delete انجام می گیرد. بعد از باز شدن صفحه ثبت کاربر جدید یا تغییر اطلاعات کاربر، صفحه زیر را مشاهده می نمایید که معنای قسمت های مختلف به صورت زیر است:

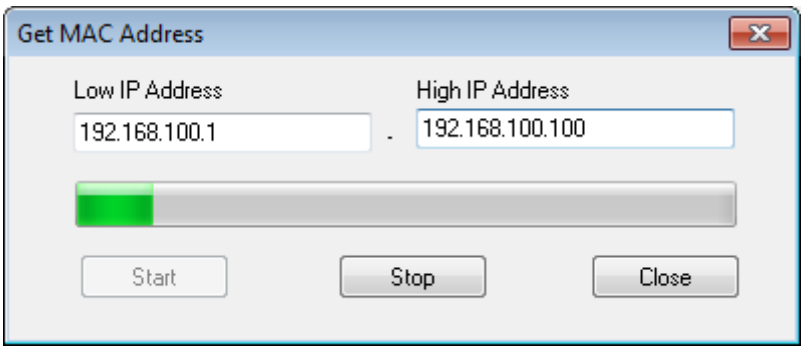
- **User/Group Name**: نام کاربر یا نام گروه می باشد.
- **Password**: اگر این گزینه تیک خورده باشد، کاربر هنگام استفاده از اینترنت، بایستی نام کاربری و رمز عبور را وارد نماید. صفحه دریافت نام کاربری و رمز عبور هر نرم افزار متفاوت بوده (مانند IE، Opera، IDM و ...) و خود نرم افزار آن ها را از کاربر دریافت می نماید.
- **IP Address/IP Range**: آدرس IP یا محدوده آدرس IP کامپیوتر هایی که کاربر می تواند از آن ها استفاده نماید.
- **MAC Address**: آدرس MAC کارت شبکه کامپیوتری که کاربر می تواند از آن استفاده نماید.
- **Enable**: فعال یا غیر فعال شدن کاربر یا گروه.
- **As Group**: اطلاعات وارد شده، مربوط به یک گروه می باشد و نه یک کاربر. این قسمت برای تعریف گروه به کار می رود. یعنی با این نرم افزار می توان کاربران را گروه بندی نمود و سیاست ها (مانند فیلتر ها و زمانبندی ها) را روی گروه ها را اعمال نمود و هر کاربری که عضو گروهی خاص شود، این سیاست ها روی وی اعمال خواهد شد.
- **Belongs to Group**: گروهی که کاربر عضو آن می باشد را مشخص می کند. با این کار دیگر امکان انجام تغییرات برای کاربر وجود ندارد و سیاست های گروه روی کاربر نیز اعمال می شود.
- **Maximum Connections**: مشخص می نماید که کاربر در هر لحظه چند درخواست اینترنتی می تواند وارد نماید (عدد ۱- به معنای بی نهایت است).
- **Download Bandwidth (KB/S)**: مشخص می نماید که کاربر حداکثر با چه سرعتی می تواند عمل دانلود و باز کردن صفحات را انجام دهد. واحد بر حسب کیلو بایت بر ثانیه می باشد (عدد ۱- به معنای بی نهایت است).
- **Upload Bandwidth (KB/S)**: مشخص می نماید که کاربر حداکثر با چه سرعتی می تواند عمل آپلود و ارسال اطلاعات را انجام دهد. واحد بر حسب کیلو بایت بر ثانیه می باشد (عدد ۱- به معنای بی نهایت است).

- **Services**: مشخص می نماید که کاربر حق استفاده از چه سرویس هایی را دارد. مثلاً www برای باز کردن صفحات وب و FTP برای کار با سرویس انتقال فایل می باشد.
- **Web Filter**: برای اعمال فیلتری خاص روی کاربر.
- **Time Schedule**: برای اعمال زمانبندی خاص روی کاربر.
- **Auto Disable At**: می توان مشخص نمود که کاربر در تاریخ و ساعت خاصی غیر فعال شود.

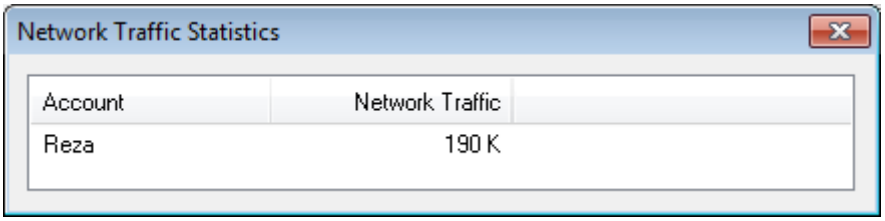


گفتیم که اگر در صفحه ایجاد کاربر جدید، کاربر را ملزم به ورود نام کاربری و رمز عبور نموده باشید، هنگامی که کاربر بخواهد از اینترنت استفاده کند، بایستی نام کاربری و رمز عبور را وارد نماید. مثلاً اگر بخواهید با Internet Explorer با اینترنت استفاده نمایید، صفحه دریافت نام کاربری و رمز عبور آن به صورت زیر می باشد:

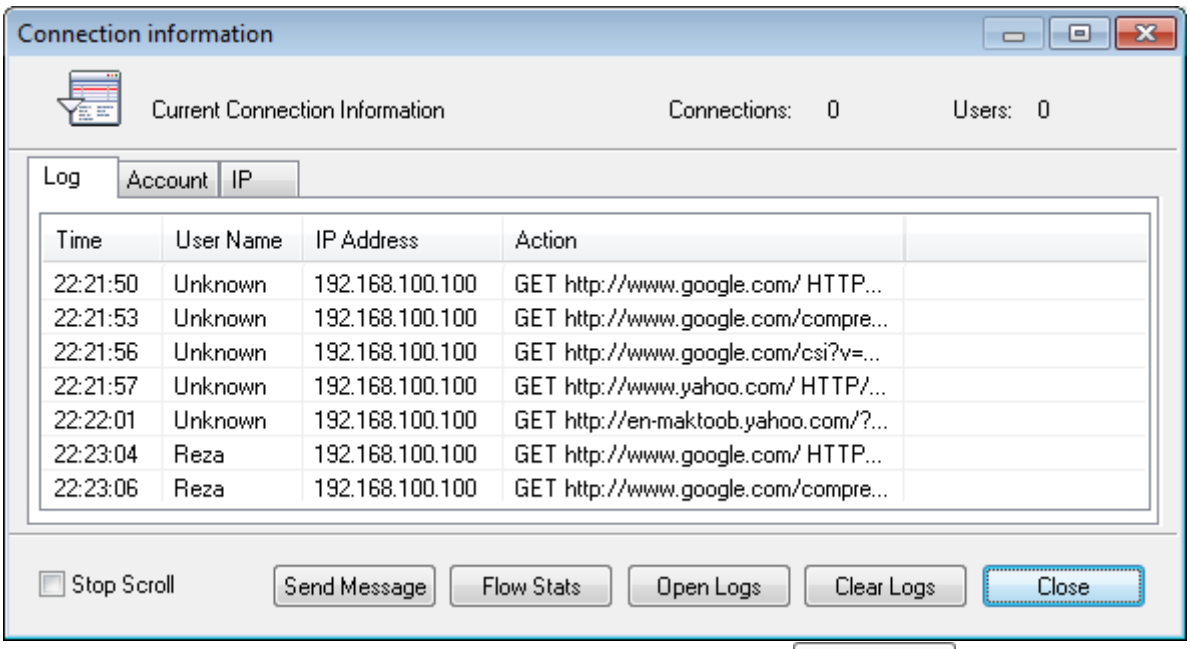
یکی دیگر از امکانات این نرم افزار، این است که می توان آدرس IP سیستم خاصی را داد و آدرس MAC آن سیستم را به دست آورد. بدین منظور، در صفحه Accounts روی دکمه Auto Scan کلیک نمایید. در صفحه باز شده، محدوده شروع و پایان جستجو را در قالب آدرس IP وارد نموده و سپس روی دکمه Start کلیک نمایید. بدین ترتیب نرم افزار دنبال کامپیوتر های موجود در محدوده وارد شده می گردد و با پیدا کردن هر کدام، آدرس MAC آن ها را به لیست کاربران اضافه می نماید.



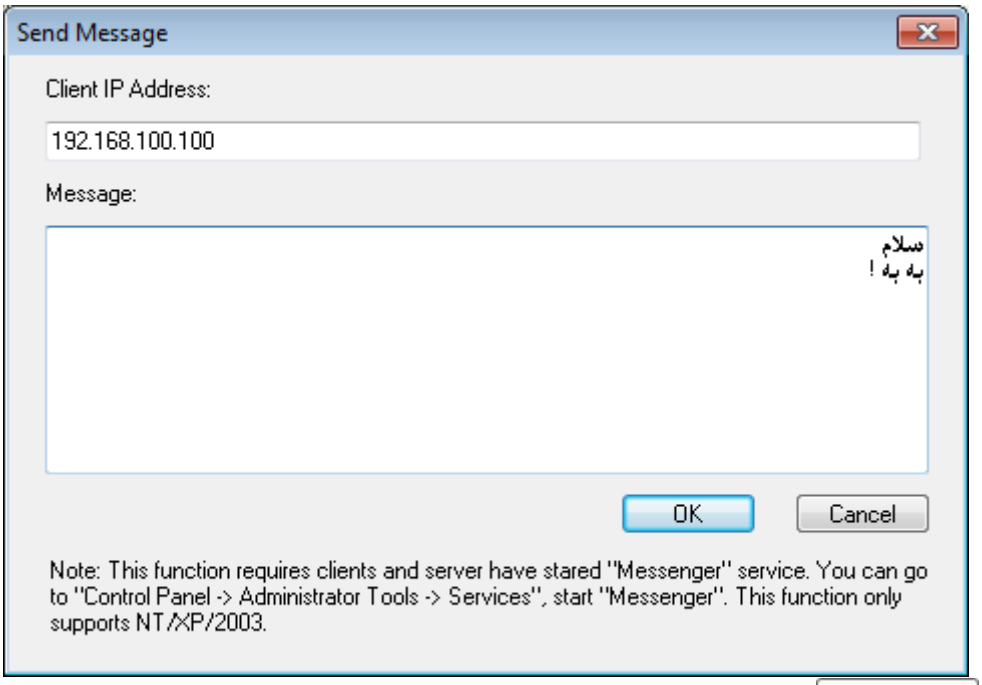
صفحه Accounts امکان دیگری که به ما می دهد، امکان مشاهده آمار ترافیک کاربران می باشد. بدین منظور در صفحه Accounts روی دکمه Flow Stats کلیک نمایید تا صفحه ای مانند صفحه زیر مشاهده کنید.



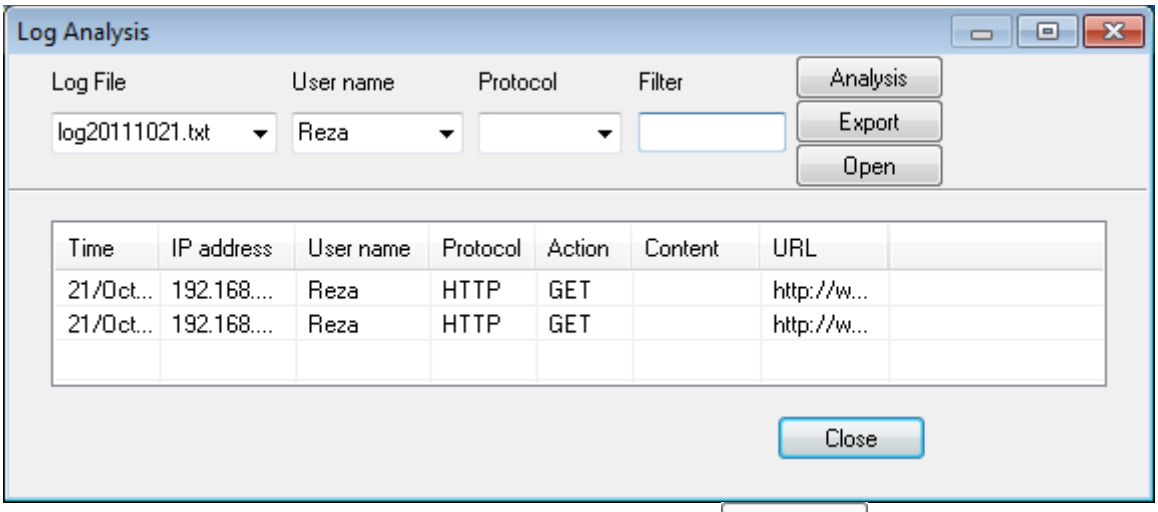
از دیگر امکانات اصلی این نرم افزار، امکان مشاهده وقایع اتفاق افتاده می باشد. بدین منظور در صفحه اصلی نرم افزار، روی دکمه Monitor کلیک نمایید. در صفحه باز شده، ۳ سربرگ مشاهده می نمایید که سربرگ Log تک تک وقایع اتفاق افتاده را نمایش می دهد.



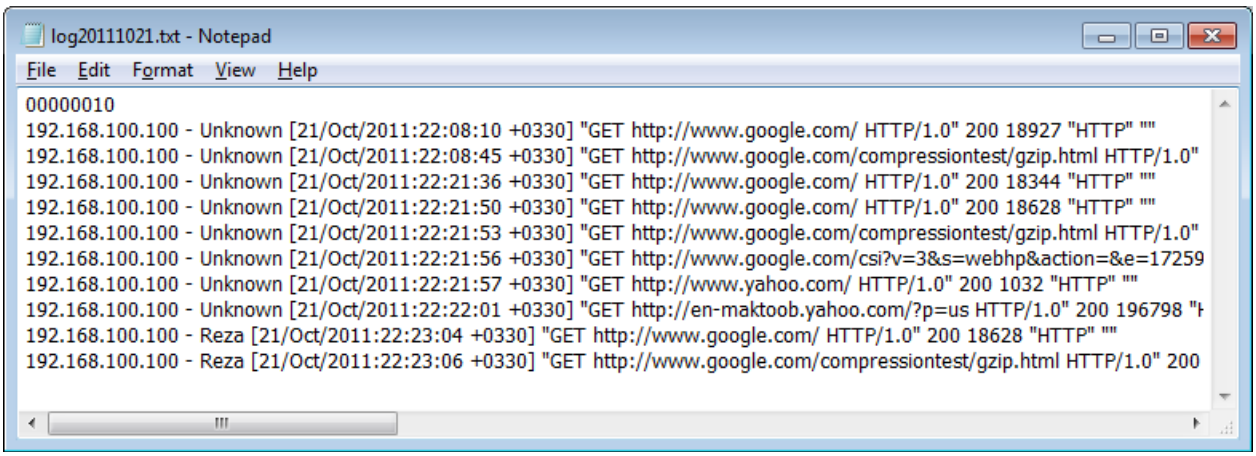
اگر در این صفحه روی دکمه Send Message کلیک کنید، صفحه ای مانند صفحه زیر باز می شود که امکان ارسال پیام به کامپیوتری خاص را به ما می دهد. البته این کار در صورتی قابل انجام است که سرویس پیام رسانی روی کلاینت ها فعال شده باشد.



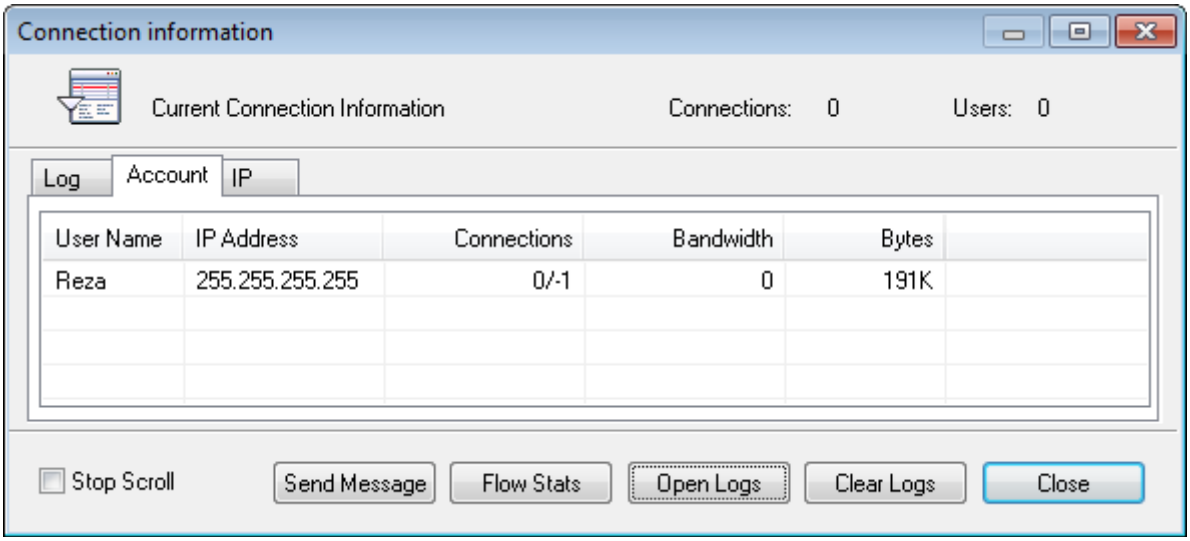
اما اگر روی دکمه Open Logs کلیک نمایید، صفحه آمارگیری و آنالیز اطلاعات باز می شود که این صفحه یکی از امکانات پر قدرت این نرم افزار می باشد. در این صفحه این امکان وجود دارد که بر اساس تاریخی خاص، کاربری خاص، پروتکلی خاص و کلمه کلیدی خاص، اطلاعات را فیلتر نمود. هر کدام از اطلاعات که وارد نشود، نرم افزار به دنبال کل اطلاعات می گردد. مثلاً اگر تاریخ وارد نشود، نرم افزار در تمامی تاریخ های موجود عمل جستجو را انجام می دهد.



در همین صفحه با کلیک روی دکمه Open می توان خود Log File را در Note Pad مشاهده نمود.

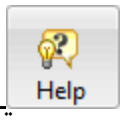


سربرگ دوم، سربرگ Account می باشد که در آن می توان حساب های موجود به همراه برخی اطلاعات آن را مشاهده نمود.



یکی دیگر از قسمت های نرم افزار، قسمت ثبت نرم افزار می باشد. برای ثبت نرم افزار، پس از خرید نرم افزار بایستی شماره سریال های داده شده را وارد نمایید. بدین منظور روی دکمه 

کلیک نمایید.

در پایان نوبت به قسمت Help یا راهنمای نرم افزار می رسد که با کلیک روی دکمه 

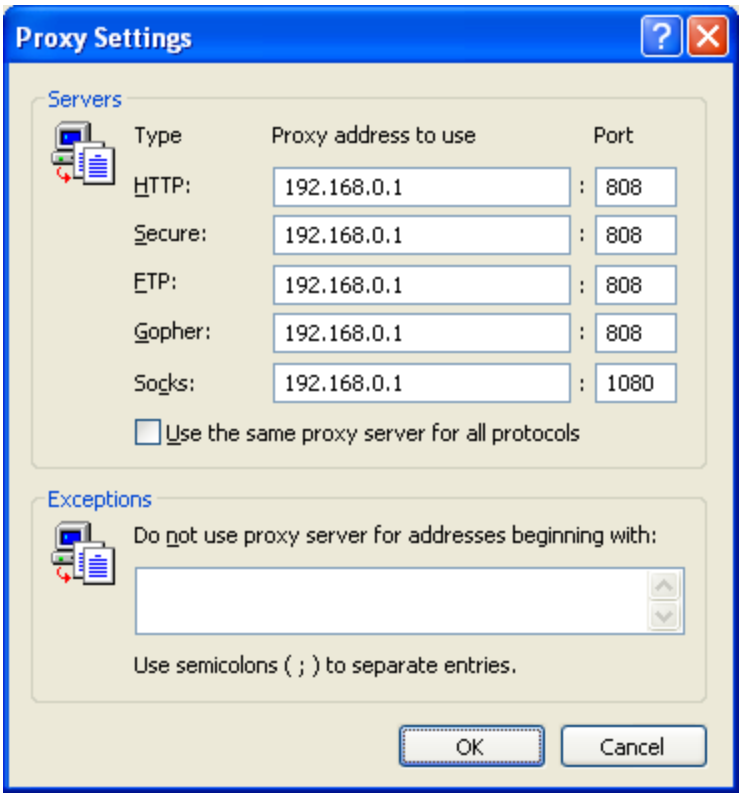
یک فایل PDF در قالب راهنمای نرم افزار باز می شود.

۱۱-۵-۲- تنظیمات کلاینت ها

تا اینجا ما توضیح دادیم که چگونه سرور را تنظیم کنیم. اما کلاینت ها نیز برای استفاده از اینترنت به اشتراک گذاشته شده نیاز به تنظیماتی خاص دارند و این تنظیمات بدین صورت می باشد که اکثر نرم افزار هایی که از اینترنت استفاده می کنند، قسمتی به نام Proxy Server دارند کا بایستی این قسمت را پیدا نمود و سپس آدرس IP سرور که نرم افزار Web Proxy روی آن نصب است به همراه شماره پورت های سرویس های مختلف را وارد نمود. در ادامه محل تنظیمات Proxy Server برخی از نرم افزار های معروف را نشان می دهیم.

Internet Explorer ←

Tools ➔ Internet Options ➔ Connections ➔ LAN settings ➔ Use a proxy server ➔ Advanced



Fire Fox ←

Tools ➔ Options➔ Advanced ➔ Network ➔ Settings

Internet Download Manager ←

Options ➔ Proxy

Outlook: هنگام ساخت حساب جدید می توان تنظیمات را وارد نمود.

Cute FTP ←

Edit ➔ Settings ➔ Connection ➔ Firewall

ICQ ←

ICQ ➔ Menu Main ➔ Preferences ➔ Connection ➔ Server ➔ Use Firewall ➔ Proxy

MSN Messenger ←

Tool ➔ Options ➔ Connection ➔ I use proxy server ➔ Type = SOCKS 5

Real Player ←

View ➔ Preferences ➔ Proxy ➔ Streaming Settings ➔ Change Settings

Windows Media Player ←

Tools ➔ Options ➔ Network ➔ Http ➔ Configure

AVG Update ←

AVG ➔ Update Manager ➔ Settings ➔ Proxy ➔ User proxy server

Windows XP Update ← اگر آدرس سرور ۱۹۲.۱۶۸.۰.۱ باشد:

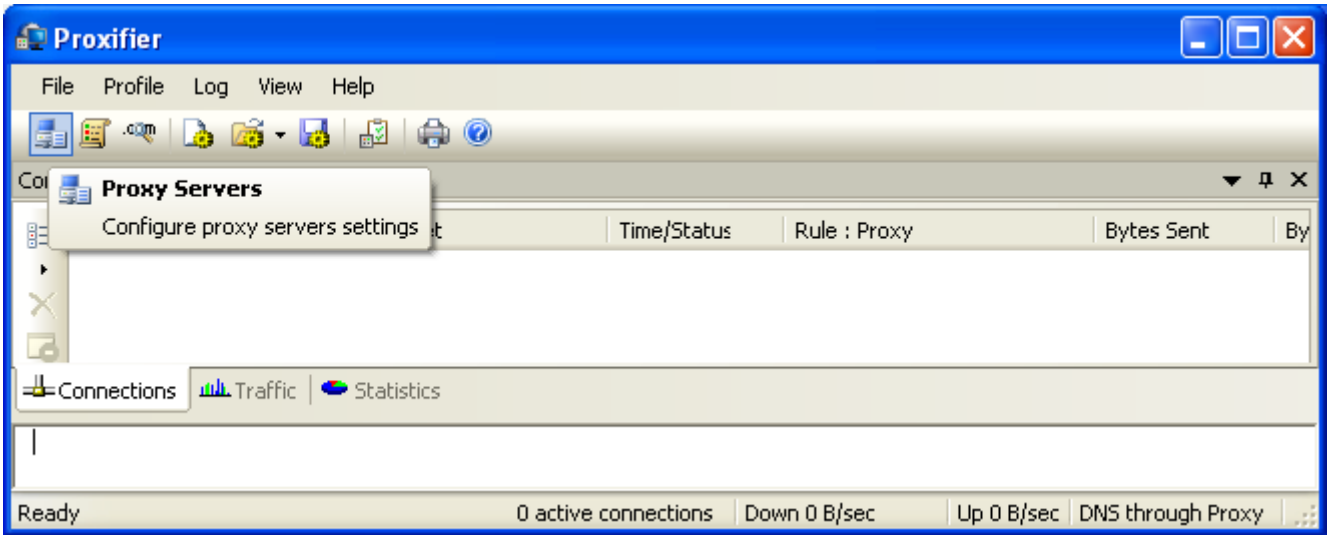
Command Prompt ➔ proxycfg -p 192.168.0.1:808

۱۱-۵-۳- نرم افزار مدیریت Client در استفاده از Proxy Server

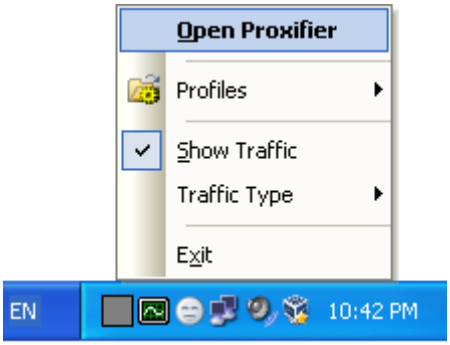
تا اینجا نحوه تنظیم کلاینت ها در مورد استفاده از Proxy Server مشخص شد. فرآیند کار بدین صورت بود که به ازاء هر نرم افزاری که می خواهد از اینترنت استفاده کند، وارد بخش تنظیمات Proxy آن می شدیم و سپس اطلاعات Proxy Server را وارد می نمودیم. اما مشکل بزرگی که در این کار وجود دارد، این است که در برخی نرم افزار ها، اصلا بخشی برای تنظیمات Proxy Server وجود ندارد. در برخی دیگر نیز انجام این تنظیمات به دلیل مسائل امنیتی بسیار سخت می باشد. در مجموع این کار راحتی نیست که برای هر بار استفاده از Proxy Server، نرم افزار های خود را تنظیم نماییم.

حالت مناسب و ایده آل این است که تنظیمات Proxy Server یک نقطه مرکزی را تغییر دهیم و با این کار، این تنظیمات روی تمامی نرم افزار هایی که از اینترنت استفاده می کنند اعمال شود؛ حتی نرم افزار هایی که قسمت تنظیمات Proxy Server را ندارند. خوشبختانه نرم افزار هایی برای انجام این کار ایجاد شده اند. نرم افزاری که در اینجا معرفی می کنیم، نرم افزار Proxifier V 3.0 است که حجم کمی دارد (حدود ۴ مگابایت) و به راحتی از اینترنت قابل دانلود می باشد (البته مانند CCProxy نیاز به Register شدن دارد). ویژگی مناسب نرم افزار Proxifier این می باشد که با انجام تنظیمات Proxy Server روی آن، از این پس هر نرم افزاری که قصد استفاده از اینترنت را داشته باشد، از این Proxy Server استفاده خواهد نمود و اینترنت خود را از Proxy Server مشخص شده دریافت خواهد کرد. مزیت دیگر این نرم افزار، قابلیت تعریف چندین Proxy Server می باشد. با این کار می توان اینترنت را همزمان از چندین Proxy Server دریافت نمود و این یعنی افزایش سرعت دسترسی به اینترنت و عدم اعمال بار زیاد روی یک Proxy Server خاص.

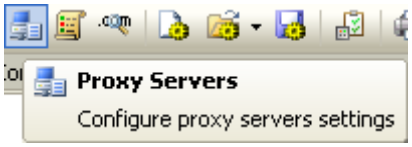
جهت استفاده از برنامه Proxifier، ابتدا آن را نصب نمایید. بعد از نصب برنامه و باز کردن آن، صفحه ای مانند صفحه زیر مشاهده خواهید نمود:



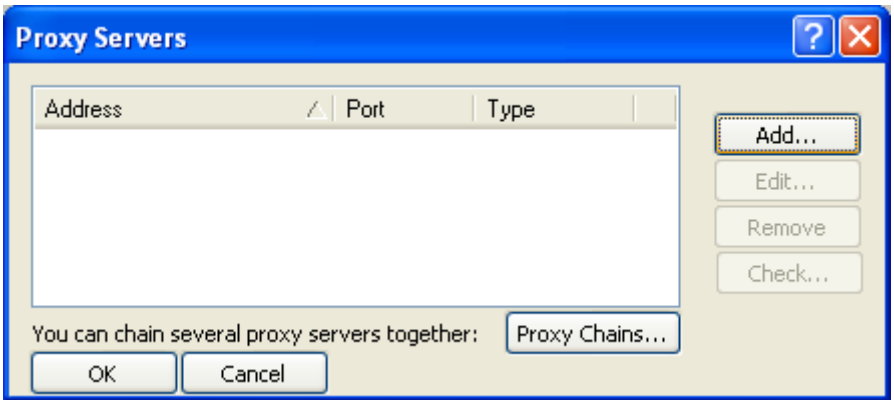
البته ممکن است که بعد از اجرای برنامه، برنامه به صورت خودکار Minimize شده و در System Try قرار گیرد. برای باز کردن آن به صورت زیر عمل نمایید:



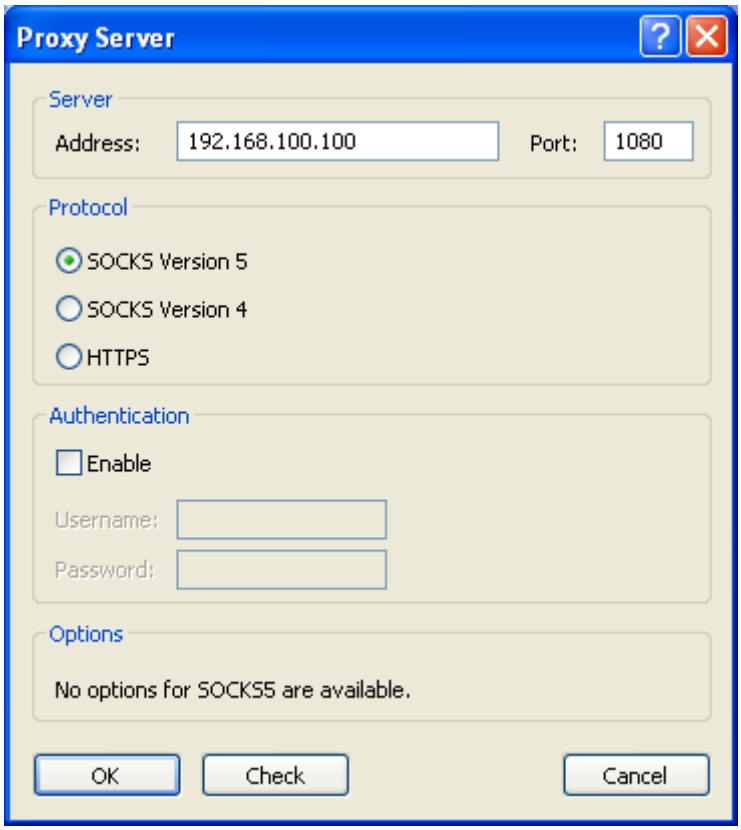
پس از باز شدن برنامه، وارد قسمت تنظیمات آن شوید. بدین منظور وارد بخش Proxy Servers شود:



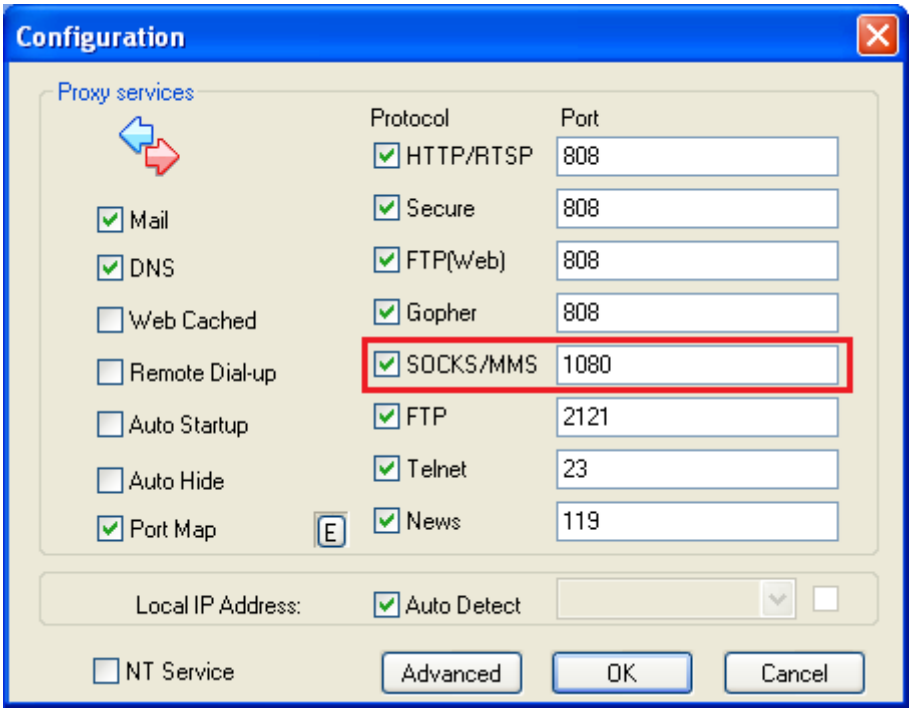
در صفحه باز شده می توانید لیستی از Proxy Server های ثبت شده را مشاهده نمایید (در این تصویر ما هنوز هیچ سروری اضافه نکرده ایم). جهت افزودن سرور جدید، روی دکمه Add کلیک نمایید.



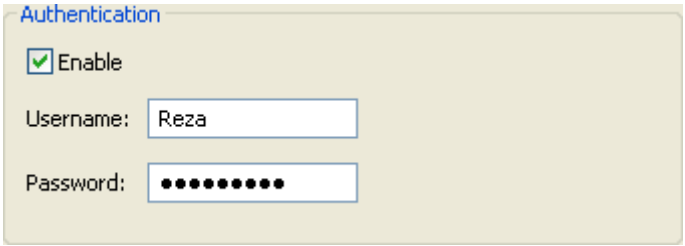
در صفحه باز شده، در قسمت Address، آدرس IP کامپیوتر Proxy Server را وارد نمایید. در قسمت Port نیز آدرس پورت SOCKS/MMS که در نرم افزار CCProxy مشخص شده است را وارد نمایید. نوع پروتکل را نیز SOCKS Version 5 انتخاب کنید.



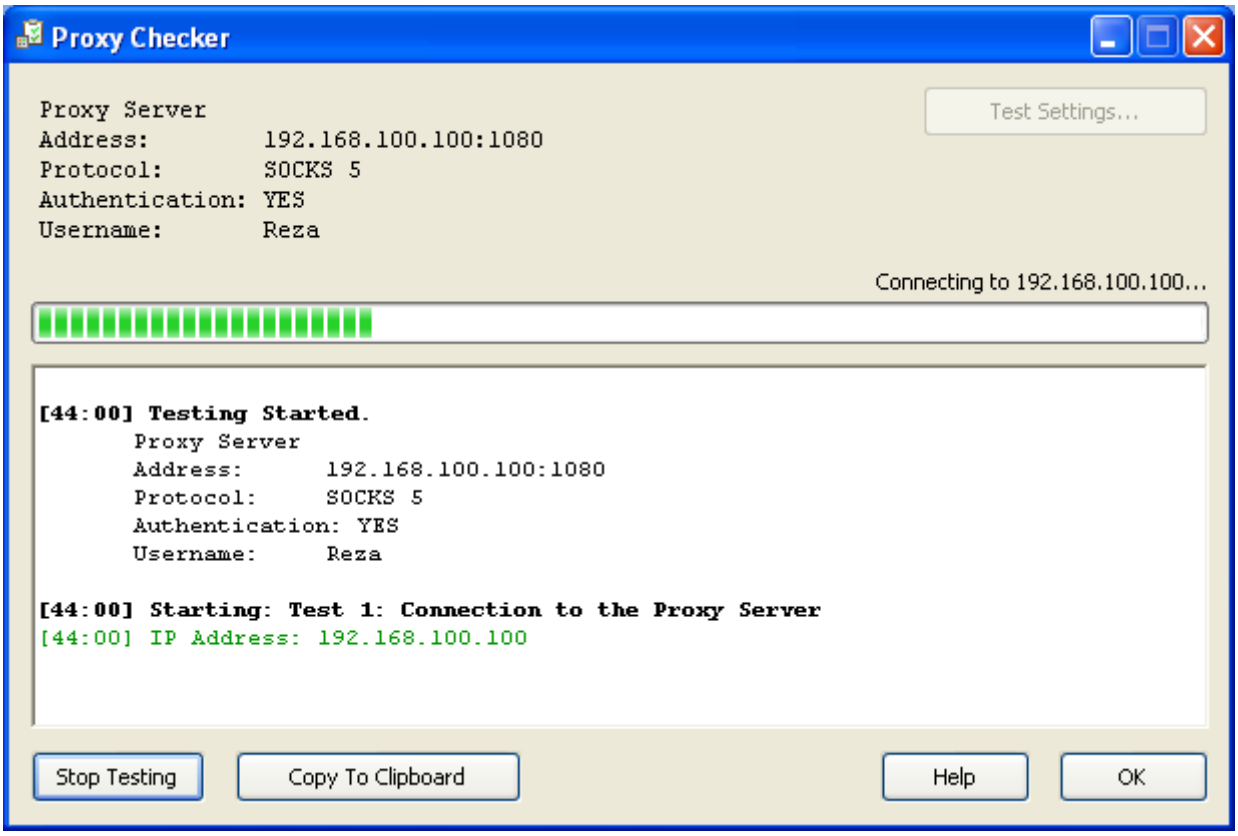
نکته بسیار مهم در شماره پورت است. **توجه: در اینجا بایستی شماره پورت SOCKS/MMS را وارد نمایید و نه شماره پورت HTTP**. برای یافتن این شماره پورت، وارد نرم افزار CCProxy شوید (همان نرم افزار سرویس پروکسی که در سرور اینترنت نصب شده است)، و از قسمت Options شماره پورت SOCKS/MMS را مشاهده نمایید. دقت فرمایید که این پورت فعال باشد.



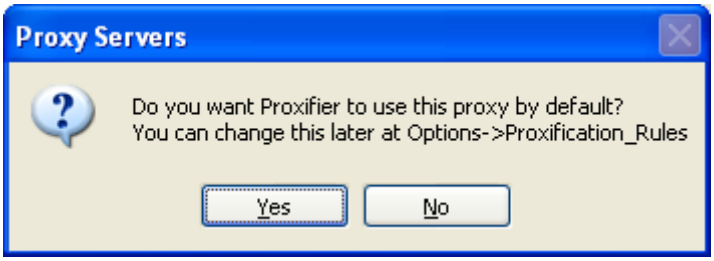
مجددا به نرم افزار Proxifier باز می گردیم. تا کنون مشخص نمودیم که سیستم ما به کدام سرور و به کدام پورت آن متصل شود؟ بحثی که باقی می ماند، تنظیم User Name و Password می باشد. اگر به یاد داشته باشید، در نرم افزار CCProxy این امکان وجود داشت که برای کاربران، User Name و Password تعریف نمود. یعنی تنها کاربرانی حق استفاده از اینترنت Share شده را داشته باشند که یک نام کاربری و رمز عبور داشته باشند. برای وارد کردن نام کاربری و رمز عبور، در نرم افزار Proxifier در همان صفحه افزودن سرور، نام کاربری و رمز عبور خود را در قسمت Authentication وارد نمایید.



اگر می خواهید از صحت تنظیمات خود مطلع شوید، در همین صفحه روی دکمه Check کلیک نمایید. با این کار صفحه کنترل صحت اتصال به Proxy Server باز می شود.



در نهایت، پس از افزودن سرور، سیستم از شما می پرسد که آیا این تنظیمات به عنوان تنظیمات پیش فرض ذخیره شود؟ سوال را تایید نماید.



با این کار، تنظیمات Proxy Server روی Client اعمال می شود و هر نرم افزاری که بخواهد از اینترنت استفاده کند، اینترنت خود را از Proxy Server تعیین شده دریافت خواهد نمود. **فقط به یاد داشته باشید که نرم افزار Proxyfier را هیچ گاه نبندید؛** زیرا با اینکار، تمامی نرم افزار ها مانند حالت معمولی از اینترنت استفاده خواهند نمود و دیگر کاری به Proxy Server نخواهند داشت.

۱۱-۶- آموزش عملی روش NAT یا ICS

در ادامه چگونگی به اشتراک گذاری اینترنت از طریق ICS را توضیح می دهیم.

سیستم مایکروسافت موسوم به ICS محدودیت تعداد کلاینت ندارند و این یکی از بارز ترین ویژگی های این سیستم هست. هرچند برای شبکه های بالای ۵ کلاینت همیشه پیشنهاد می شود تا از سیستم های سروری (Proxy Server) استفاده کرد، اما ICS توانایی کنترل شبکه های کوچک را به خوبی دارد.

روش پیاده سازی ICS در تمام شبکه ها یکسان است، پس با این حساب اصلا مهم نیست شبکه شما Wireless هست یا سیمی، با اینکه اینترنت شما چگونه به دست شما میرسد.

۱۱-۶-۱- شروع به کار

شما از هر طریقی که اینترنت را دریافت کنید، (چه Wireless چه ADSL چه ISDN و...) سر انجام باید کارت شبکه ای به آن اختصاص یافته باشد.

نکته: گاهی پیش می آید که مودم های ADSL از طریق پورت USB به سیستم متصل می شوند، اما اگر دقت کنید در بخش تنظیمات ویندوز برای آن نیز یک کارت شبکه (حتی به صورت مجازی) وجود دارد.

نکته: در بعضی از مودم های ADSL که امروزه وجود دارند تنظیمات از طریق Connectionهایی مانند Dial-up تنظیم می شوند که البته بازهم تاثیری در روند کار ندارد. شما آن را به حکم یک کارت شبکه بشناسید.

نکته: برای ICS اصلا لزوم داشتن IP Public (به اصطلاح عامیانه Valid) یا Static وجود ندارد.

سرور: در بحث Share کردن اینترنت، سرور را به کامپیوتری خواهیم گفت که یک ویندوز XP بر روی آن نصب شده و قرار است کار اشتراک گذاری اینترنت را برای کلاینت ها انجام دهد. (این لفظ به معنای این نیست که شما یک ویندوز سرور احتیاج دارید)

شما برای شبکه خود مجبور هستید از یک کارت شبکه استفاده کنید (بسته به شبکه سیمی یا بی سیم). پس شما دو کارت شبکه در سرور خواهید داشت.

۱. کارت شبکه ای که اینترنت به آن وصل شده است. (به نکته اول و دوم در همین صفحه دقت کنید)

۲. کارت شبکه ای که به شبکه داخلی متصل است. (حال می تواند این شبکه فقط یک کامپیوتر دیگر باشد.)

کارت شبکه اینترنت: این لفظ را از این پس در مورد کارت شبکه ای به کار می بریم که به اینترنت متصل است.

کارت شبکه داخلی: این لفظ را از این پس در مورد کارت شبکه ای به کار می بریم که به شبکه داخلی (یا کامپیوتر مجاور به هر طریقی) متصل است.

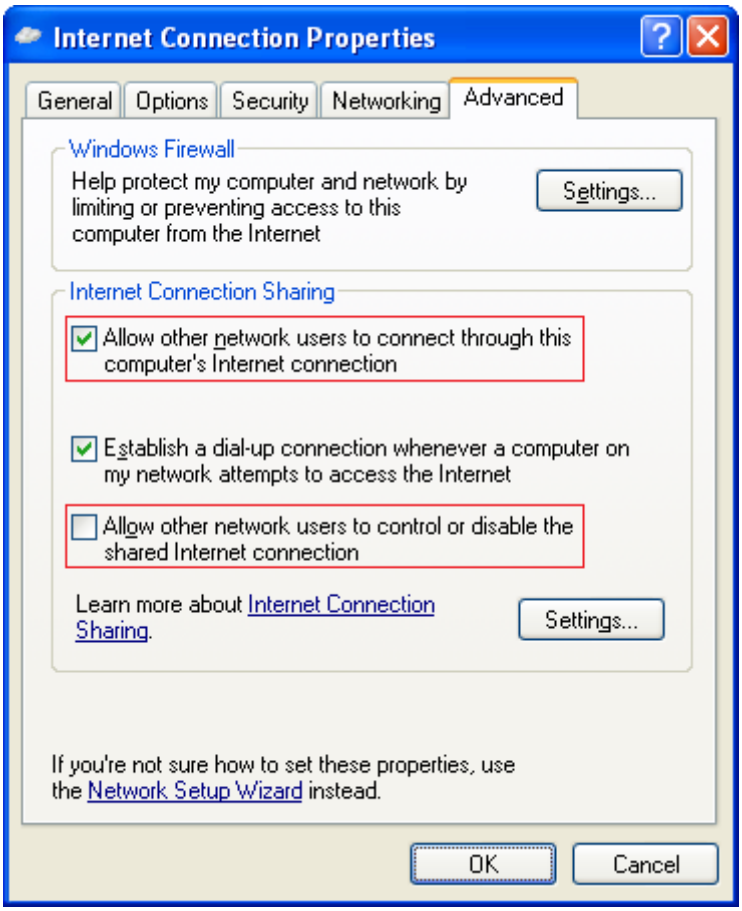
۱۱-۶-۲- مراحل راه اندازی

۱. از Control Panel وارد Network Connection شوید.

۲. بر روی کارت شبکه اینترنت راست کلیک کنید و سپس گزینه Properties را کلیک کنید.

۳. از سربرگ های موجود، سربرگ Advanced را انتخاب کنید. (در ویندوز ویستا و ویندوز ۷، این سربرگ به Sharing تغییر نام پیدا کرده است)

۴. در صفحه موجود در بخش Internet Connection Sharing، تیک Allow other network users to connect through this computer's Internet connection تا بزنید.



چند نکته که در راه اندازی ICS باید آنرا حتما رعایت کنید :

- اگر از چند کارت شبکه در کامپیوتر استفاده می کنید، شما می توانید از ICS تنها برای یک کارت شبکه داخلی استفاده کنید. در این صورت از منوی Home Networking Connection شبکه مورد نظر را انتخاب کنید.
- اگر به اعضای (کلاینت) شبکه اطمینان ندارید، تیک Allow other network users to control or disable the Shared internet connection را حتما بردارید.

مرحله مهم: بعد از فعال شدن ICS، کارت شبکه داخلی (همانی که قرار است از اینترنت Share شده استفاده کنند) و تمام کارت شبکه هایی که قرار است از اشتراک اینترنت استفاده کنند را در حالت Obtain an IP Address Automatically قرار دهید.

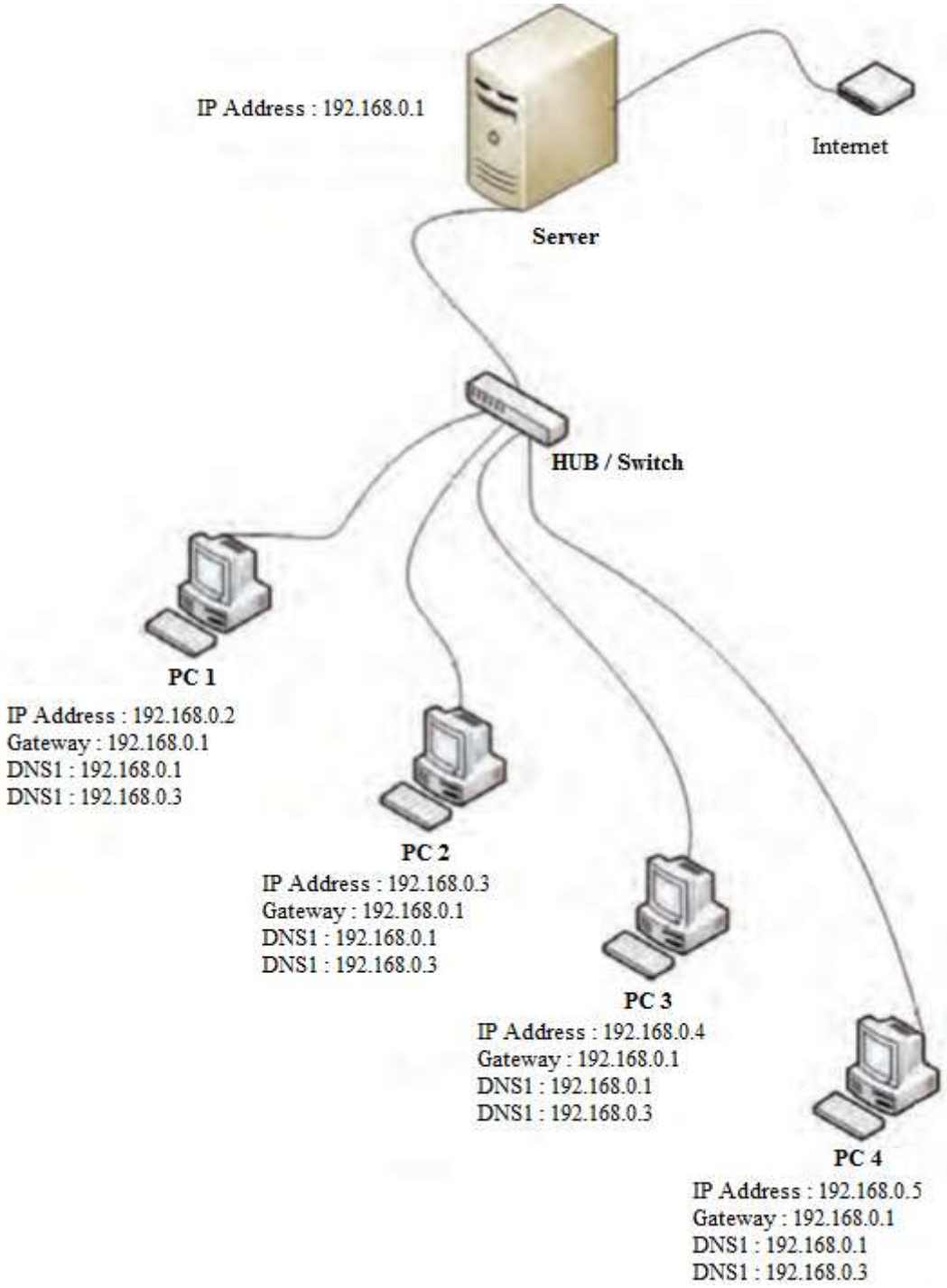
حال کارت شبکه داخلی خود را یک بار خاموش/روشن کنید (Disable/Enable) کرده و منتظر باشید که کارت شبکه IP بگیرد (اگر حالش را ندارید، کامپیوتر کلاینت را یکبار Restart کنید).

نکته: مطمئن شوید در صورتی که کارت شبکه های متفاوتی در سیستم دارید هیچ کدام از محدوده ۱۹۲.۱۶۸.۰.۰ نباشند. کارت شبکه اینترنت شما در سرور حتما باید آدرس ۱۹۲.۱۶۸.۰.۱ را بگیرد (این کار به صورت خودکار انجام می گیرد) و به این ترتیب خود به بقیه کارت شبکه ها نیز IP می دهد که تماما از همین محدوده هستند. **البته اگر می خواهید آدرس دهی IP به صورت خودکار صورت نگیرد، IP کامپیوتر سرور را به صورت دستی تنظیم نمایید، سپس در کامپیوتر هایی که می خواهید از اینترنت استفاده کنند، آدرس Default Gateway آن ها را برابر با آدرس سرور قرار دهید (یعنی اگر آدرس سرور به صورت خودکار به ۱۹۲.۱۶۸.۰.۱ تغییر یافت، تمامی کلاینت ها نیز بایستی آدرس Gateway خود را به ۱۹۲.۱۶۸.۰.۱ تغییر دهند).** به یاد آورید که با تنظیم Gateway به سیستم می گفتیم که تمامی درخواست های خود را به سمت این کامپیوتر بفرستد.

به همین ساده گی اینترنت به صورت کامل به اشتراک گذاشته شد.

نکته: ممکن است در شروع کار ICS کمی کندی در روند اشتراک گذاری اینترنت مشاهده شود که به مرور زمان حل خواهد شد. (گاهی اوقات زمان زیادی می برد تا یک سایت باز شود و شما مجبور هستید بارها Refresh بزنید، اما مطمئنا پس از مدتی به صورت روان فعالیت خواهد کرد.)

شکل زیر، روند اشتراک گذاری اینترنت را بهتر نشان می دهد:



فصل ۱۲

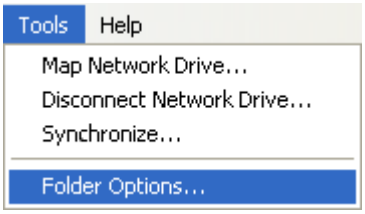
امنیت فایل ها و پوشه ها

۱۲-۱- انواع امنیت

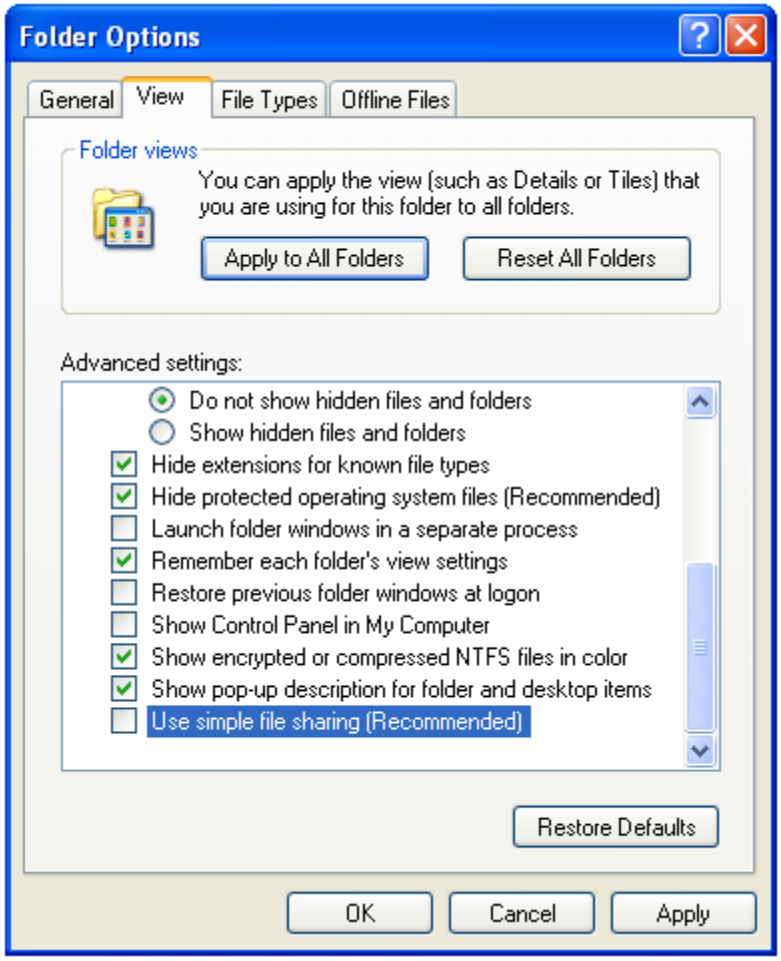
در فصل "راه اندازی شبکه های Workgroup" با نحوه به اشتراک گذاری اطلاعات و نیز نحوه ایجاد امنیت روی فایل های Share شده آشنا شدید. به عنوان مثال تعیین نمودید که در دسترسی به یک پوشه به نام TestFile، کاربری به نام Ali هیچگونه محدودیتی نداشته باشد، اما کاربری به نام Reza، فقط قابلیت دسترسی Read Only داشته باشد و قابلیت تغییر محتوای این پوشه را نداشته باشد. حال کاری که در عمل رخ می داد این بود که این محدودیت روی کاربر Reza فقط در حالت Sharing اعمال می شد. بدین معنا که اگر کاربر Reza به صورت محلی به سیستم Login می کرد، قابلیت تغییر پوشه TestFile را داشت. اما اگر کاربر Reza از طریق شبکه و به صورت Remote بخواهد به گوشه Share شده دسترسی داشته باشد، در اینصورت فقط قابلیت مشاهده پوشه را خواهد داشت؛ اما قابلیت تغییر اطلاعات این پوشه را ندارد. به عبارت دیگر این محدودیت در حالت Remote اعمال می شود و در حالت دسترسی Local این محدودیت اعمال نخواهد شد. اما در این فصل قصد داریم، گامی فراتر از این سطح امنیت برداریم و امنیت پوشه ای خاص (مثلاً TestFile) را به گونه ای تعیین نماییم، که کاربری به اسم Reza، چه به صورت Local و چه به صورت Remote خواست از این پوشه استفاده کند، یا قابلیت بازکردن پوشه را نداشته باشد یا فقط بتواند آن را به صورت Read Only باز کند.

۱۲-۲- تنظیمات امنیتی

برای رسیدن به این هدف (ایجاد تنظیمات امنیتی روی پوشه)، در گام اول بایستی تنظیمات Sharing & Security را در ویندوز XP فعال کنید. (این تنظیم در ویندوز سرور به صورت پیش فرض فعال است). بدین منظور ابتدا وارد My Computer شده، سپس از منوی Tools گزینه Folder Option را انتخاب نمایید.



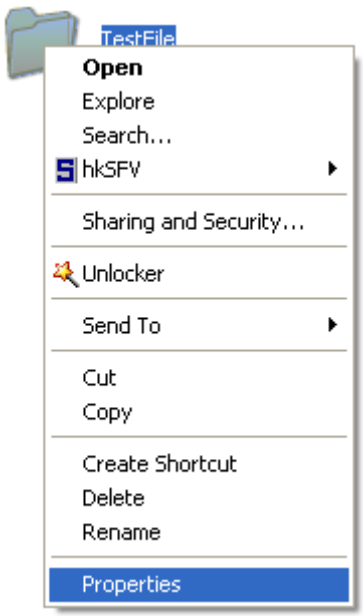
سپس وارد سربرگ View شده و سپس تیک گزینه آخر یعنی گزینه Use Simple File Sharing را بردارید.



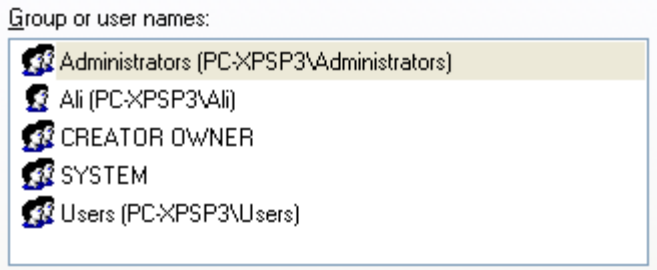
حال نوبت به ایجاد امنیت روی پوشه ای به نام TestFile می شود.

فرض کنید در این پوشه، فایلی به نام Sample Text.txt ایجاد کرده ایم تا تاثیر حالت امنیت Read Only را ببینیم.

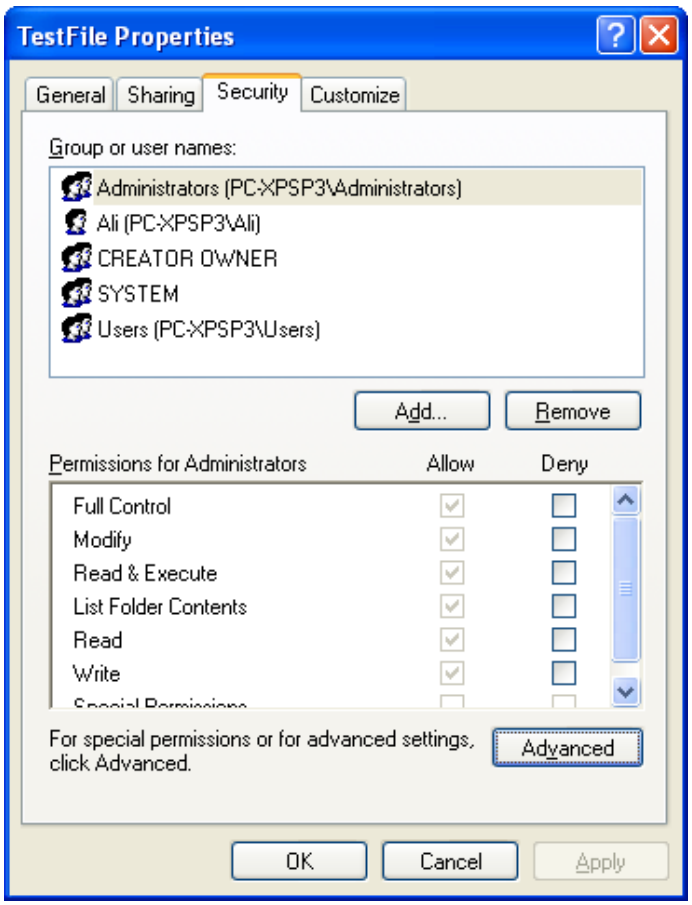
حال برای ایجاد امنیت، روی پوشه مورد نظر راست کلیک کرده و گزینه Properties را انتخاب کنید. (توجه: روی پوشه راست کلیک کنید و نه روی فایل، البته این امنیت گذاری روی فایل نیز جواب می دهد.)



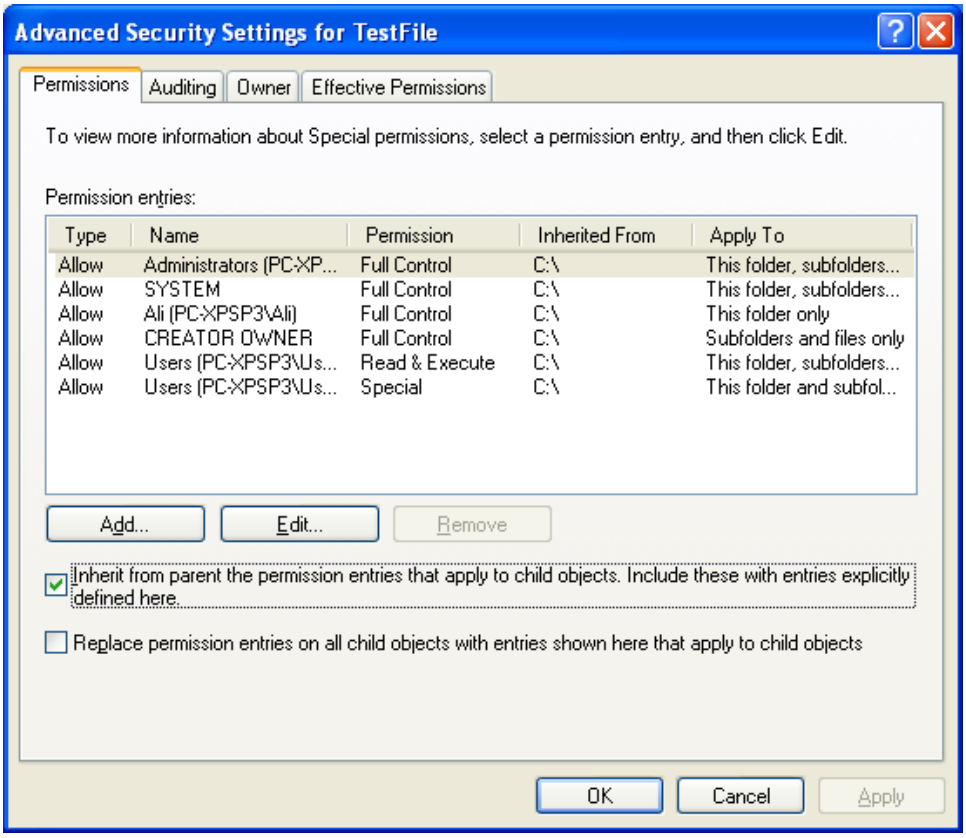
در صفحه باز شده، در بالای صفحه اسامی کاربرانی که دسترسی آن ها به این پوشه اجازه داده شده است (Allow) یا دسترسی آن ها منع شده است (Deny) را مشاهده می نمایید.



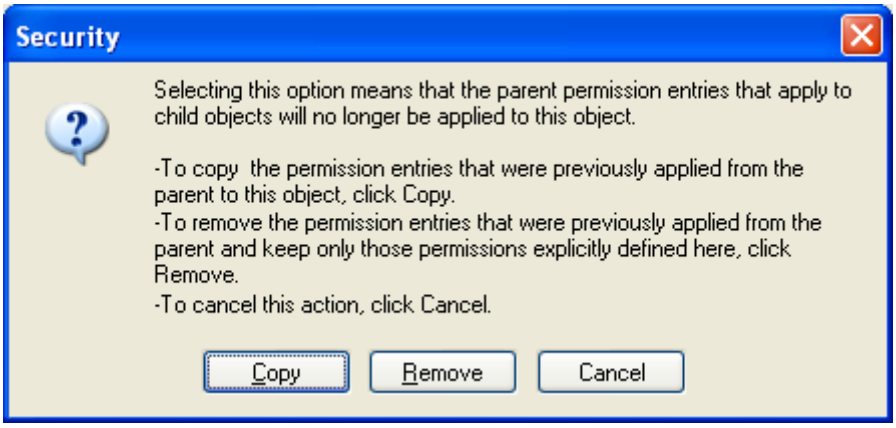
برای ایجاد امنیت روی دکمه Advanced کلیک کنید.



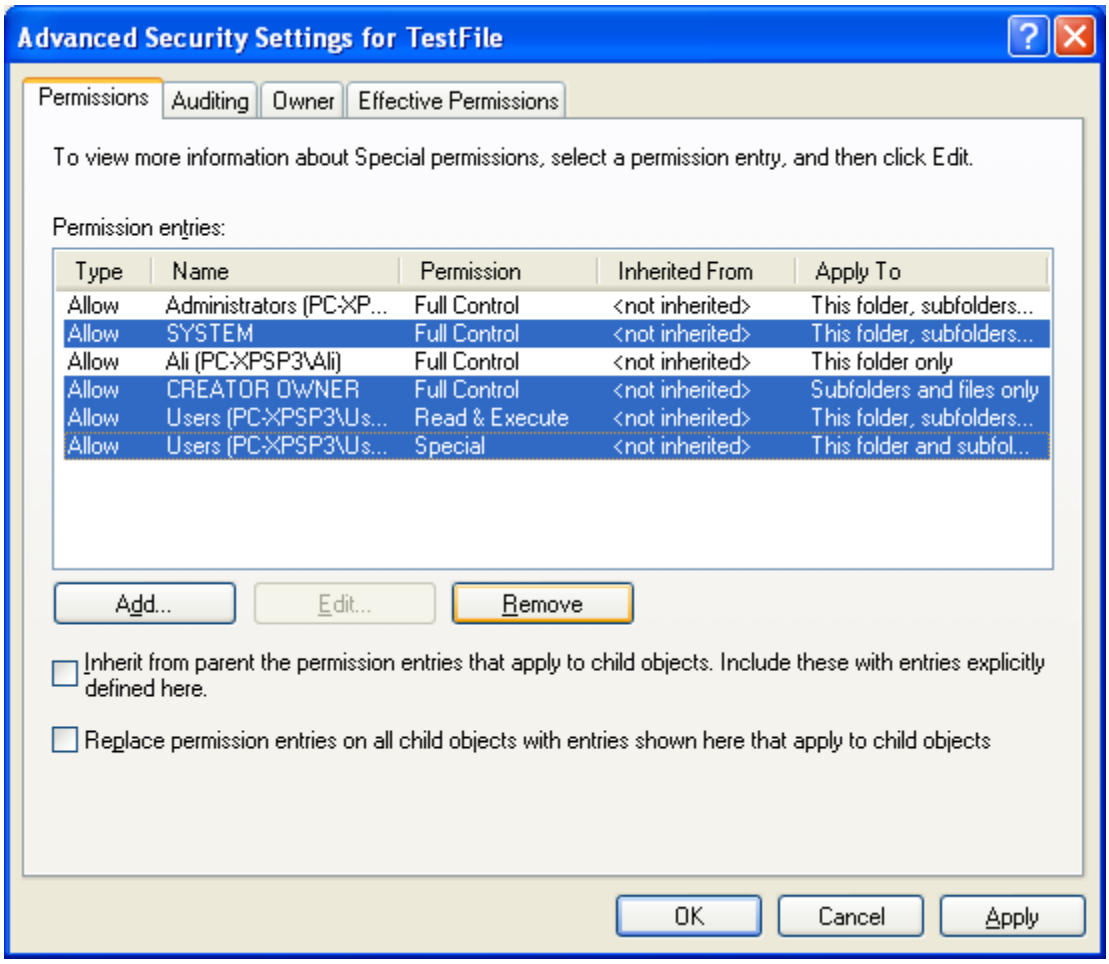
در صفحه باز شده، شما مجددا لیست دسترسی ها را با ظاهری متفاوت مشاهده خواهید نمود. در مرحله اول ابتدا تیک گزینه Inherit from parent the permission … را بردارید.



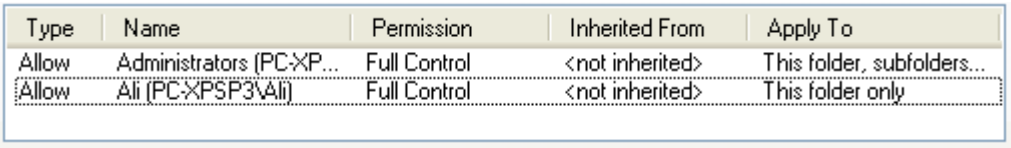
در سوالی که از شما می پرسد، گزینه Copy را انتخاب نمایید. در این صفحه، سیستم به شما می گوید که تنظیمات امنیتی را از حالت ارث بری برداشته (ارث بری را در انتهای فصل توضیح داده ایم) و سپس آن تنظیمات را به خود پوشه نسبت دهید (کپی کنید).



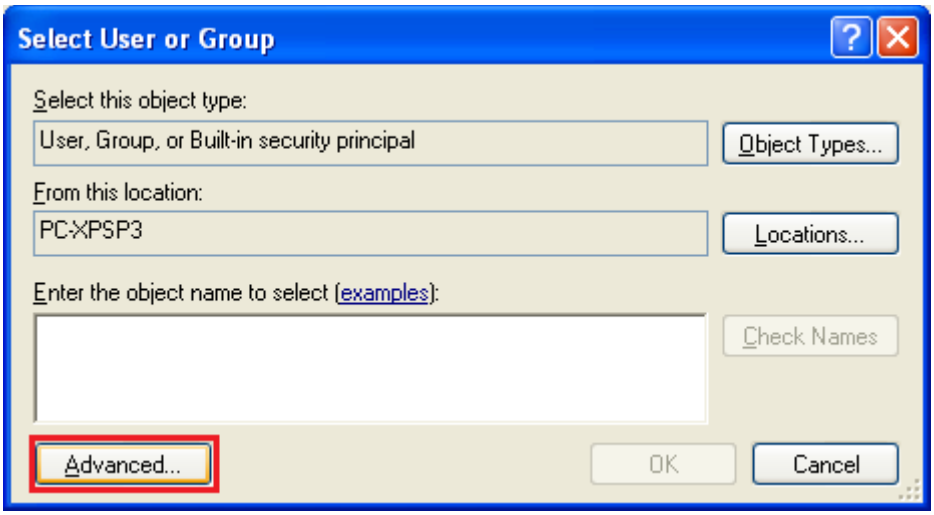
در صفحه تنظیمات دسترسی، فقط کاربرانی که می خواهید به این پوشه دسترسی داشته باشند را حفظ کرده و بقیه را حذف نمایید. بدین منظور کاربرانی که می خواهید حذف کنید را انتخاب کرده و سپس روی دکمه Remove کلیک کنید. در این مثال، ما فقط دو کاربر Ali و Administrator را نگه داشته و بقیه را حذف کرده ایم.



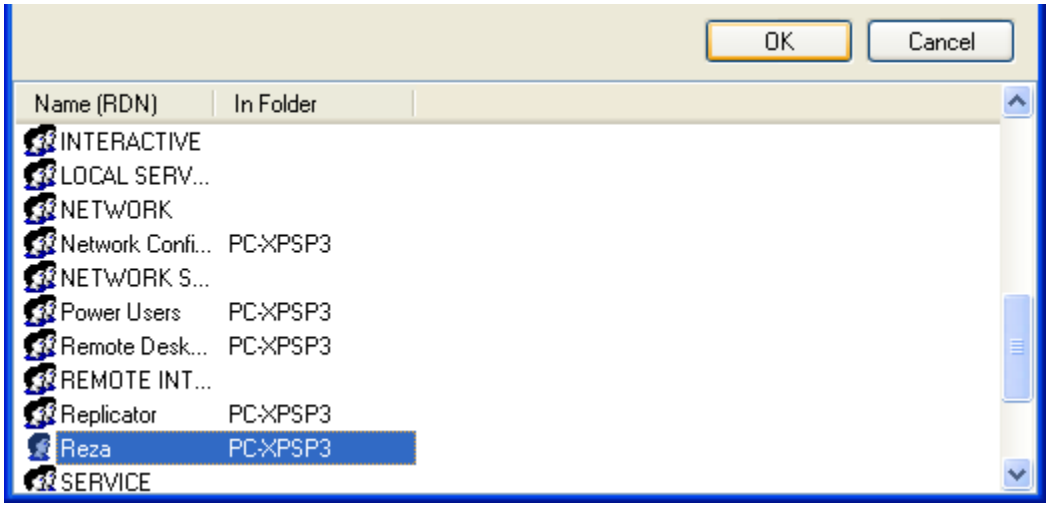
پس از OK کردن، مشاهده خواهید کرد که فقط دو کاربر Ali و Administrator باقی می مانند.



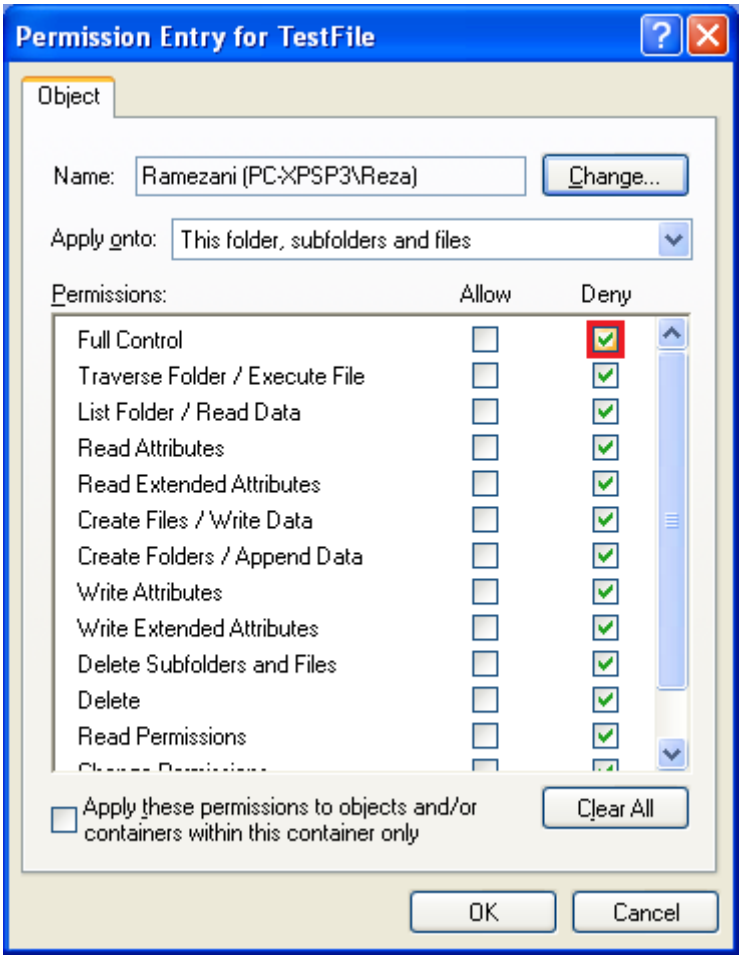
حال می خواهیم دسترسی کاربری مانند Reza را از این پوشه بگیریم. بدین منظور در همین صفحه ابتدا روی دکمه Add کلیک کنید. در صفحه باز شده برای انتخاب کاربر Reza، روی دکمه Advanced کلیک کنید.



در صفحه باز شده، ابتدا روی دکمه Find کلیک کنید تا لیست تمام کاربران به نمایش درآید. سپس کاربر Reza را انتخاب کرده و سپس دو مرتبه روی OK کلیک کنید.



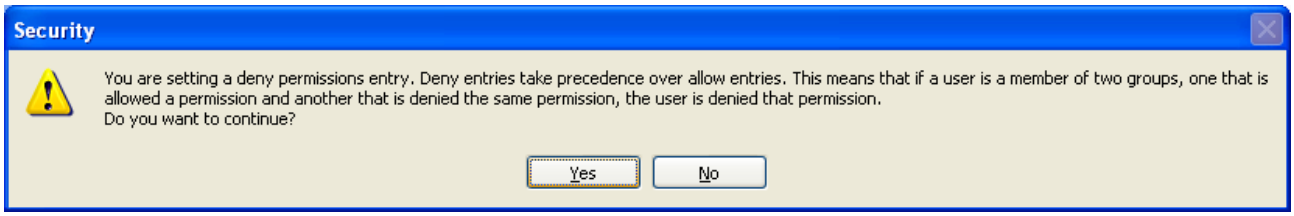
پس از OK کردن، صفحه ای مانند صفحه زیر نمایان می شود که در آن می توانید سطح دسترسی کاربر Reza را تعیین نمایید. در این صفحه دو کلمه دارید به نام Allow و Deny. ستون Allow برای دادن اجازه دسترسی و ستون Deny گرفتن اجازه دسترسی است. در این مثال ما گزینه Full Control را روی Deny تنظیم کرده ایم. بدین معنی که کاربر Reza هیچگونه دسترسی به این گوشه ندارد. در نهایت روی OK کلیک کنید.



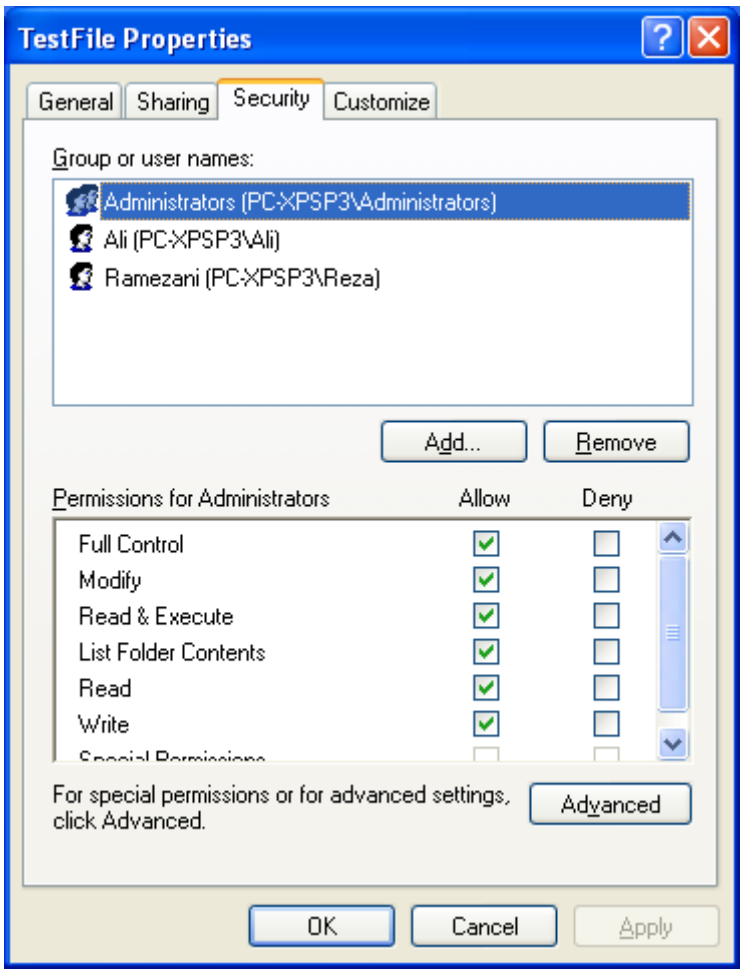
سپس مشاهده خواهید کرد که کاربر Reza نیز به لیست زیر و با نوع دسترسی Deny اضافه می شود. مجددا OK کنید.

Type	Name	Permission	Inherited From	Apply To
Deny	Ramezani (PC-XPSP...	Full Control	<not inherited>	This folder, subfolders...
Allow	Administrators (PC-XP...	Full Control	<not inherited>	This folder, subfolders...
Allow	Ali (PC-XPSP3\Ali)	Full Control	<not inherited>	This folder only

پس از OK کردن، سیستم از شما سوالی می پرسد؛ روی Yes کلیک کنید.

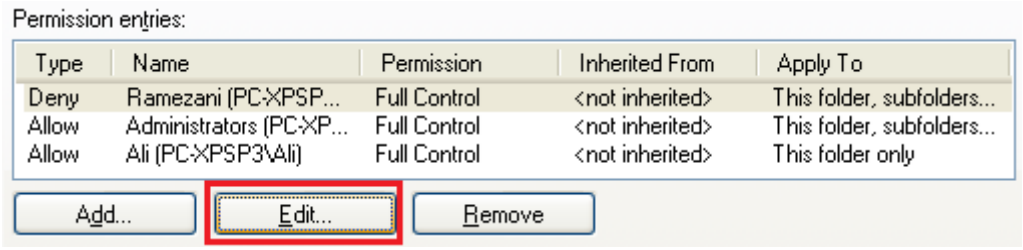


حال می بینید که کاربر Reza به لیست کاربران این پوشه اضافه می شود. در این صفحه هم کاربرانی که دسترسی Allow و هم کاربرانی که دسترسی Deny دارند را مشاهده می کنید. مجددا روی OK کلیک کنید.

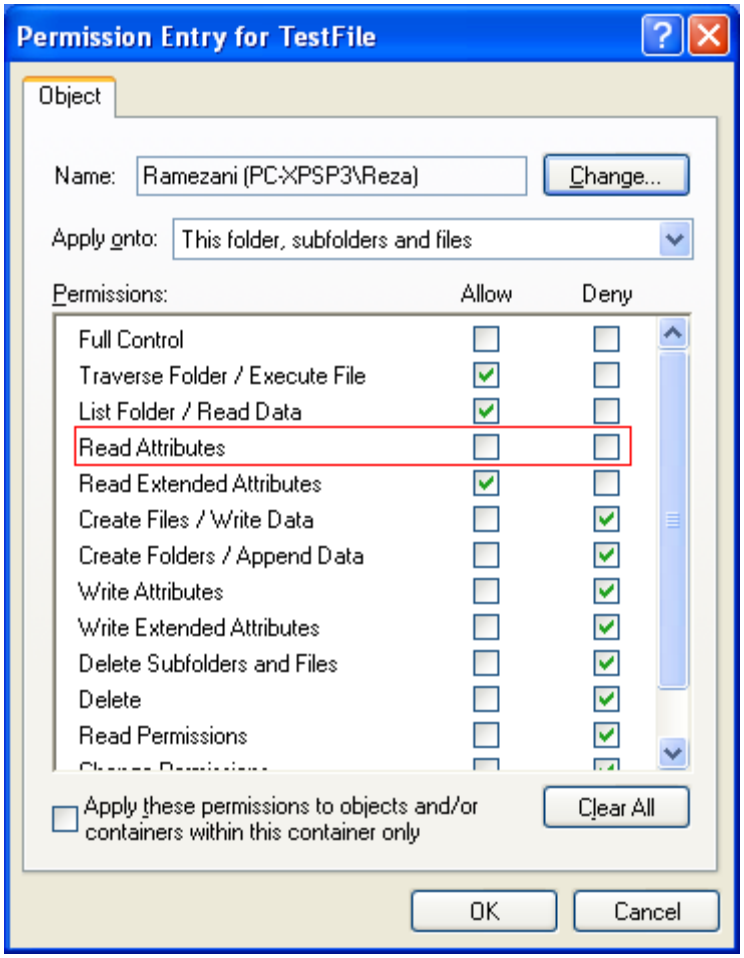


حال نوبت به دیدن تاثیر این سطح دسترسی می رسد. بدین منظور ابتدا از سیستم Log Out کرده و با کاربر Reza به سیستم Login کنید. مشاهده خواهید نمود که هنگام ورود به این پوشه، سیستم اجازه ورود شما را خواهد گرفت و پیام Access is Denied را مشاهده خواهید نمود.

حال می خواهیم به کاربر Reza اجازه دسترسی بدهیم، اما به صورت Read Only. بدین منظور از سیستم Log Out کرده و با کاربر Ali مجددا به سیستم Log In کنید. وارد صفحه تنظیمات امنیتی پوشه TestFile شده، کاربر Reza را انتخاب کرده و روی Edit کلیک کنید.



در صفحه باز شده فقط گزینه های مربوط به "دسترسی خواندنی" را Allow کرده و بقیه دسترسی هایی که مربوط به عملیات ویرایشی است را Deny کنید. اگر به شکل دقت کنید، گزینه Read Attributes نه در حالت Allow قرار دارد و نه در حالت Deny. حال به نظر شما سیستم کدام حالت را انتخاب می کند؟ جواب این است که سیستم از حالت **ارث بری** استفاده می کند. بدین معنی که فرض کنید این پوشه در ریشه درایو C:\ قرار دارد. حال اگر درایو C:\ برای دسترسی Read Attributes، حالت Allow را انتخاب کرده باشد، حالت Allow برای این پوشه نیز اعمال خواهد شد؛ در غیر اینصورت حالت Deny روی این گوشه اعمال خواهد شد.



توجه نمایید که در این روش امنیت گذاری، کاربر Reza چه به صورت محلی و چه به صورت راه دور به سیستم Login کنید، این محدودیت روی وی اعمال خواهد شد. بر عکس حالت امنیت Sharing که فقط در حالت دسترسی به فایل Share شده و از راه دور اعمال می شود.

فصل ۱۳

نرم افزار NetMeeting

فرض کنید که شبکه محلی خود را راه اندازی کرده ایم. اما آیا کاربرد شبکه، فقط به اشتراک گذاری منابع است؟ آیا کاربران نمی توانند به صورت Online با یکدیگر ارتباط برقرار کنند؟ جواب کاملاً مشخص است. جواب شما چیست؟

یکی از نرم افزارهایی که برای برقراری ارتباط در شبکه به کار می رود، نرم افزار NetMeeting است. این نرم افزار به صورت رایگان و توسط Microsoft به همراه ویندوز XP عرضه شده است. از این نرم افزار برای چت کردن از طریق شبکه یا نمایش دسکتاپ یک کامپیوتر دیگر استفاده می شود.

در ادامه فصل، به آموزش این نرم افزار می پردازیم.

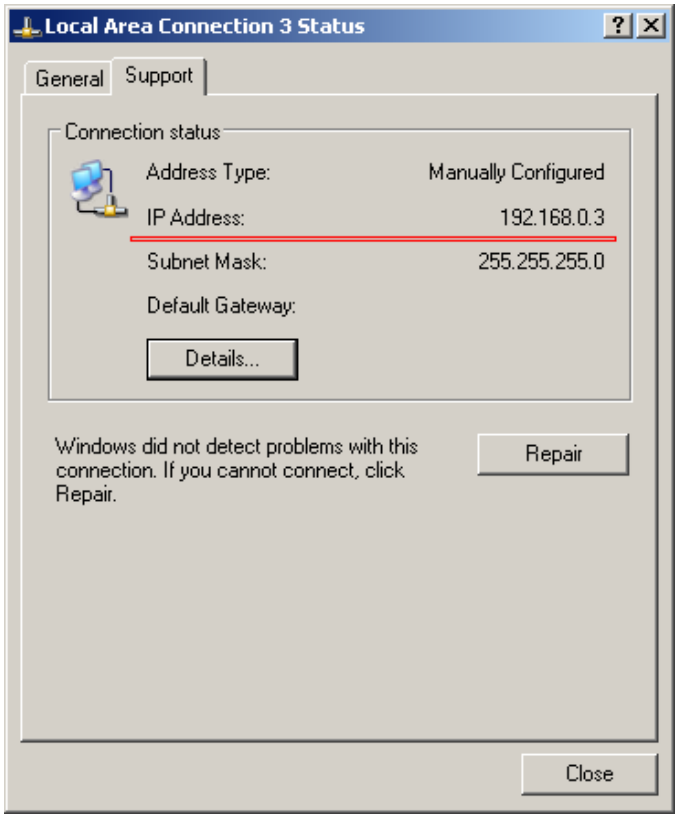
برای این کار بایستی این نرم افزار را هم در Client و هم در Server اجرا کنیم. البته این مفهوم Client و Server با مفهوم Client و Server واقعی در شبکه متفاوت است. در این مبحث منظور از Server، کامپیوتری است که صفحه دسکتاپ آن را دیگران مشاهده خواهند کرد. همچنین منظور از Client نیز، کامپیوتر هایی هستند که صفحه دسکتاپ Server را مشاهده خواهند کرد.

۱۳-۱- مشاهده آدرس IP در سرور

پس از اجرای برنامه، Client ها بایستی به Server متصل شوند. برای این اتصال، Clientها به آدرس IP مربوط به Server نیاز دارند. برای پیدا کردن آدرس IP مربوط به Server، بر روی خود Server مراحل زیر را دنبال نمایید:

۱- بر روی آیکون کارت شبکه که در سمت راست نوار وظیفه قرار دارد، دو بار کلیک نمایید.

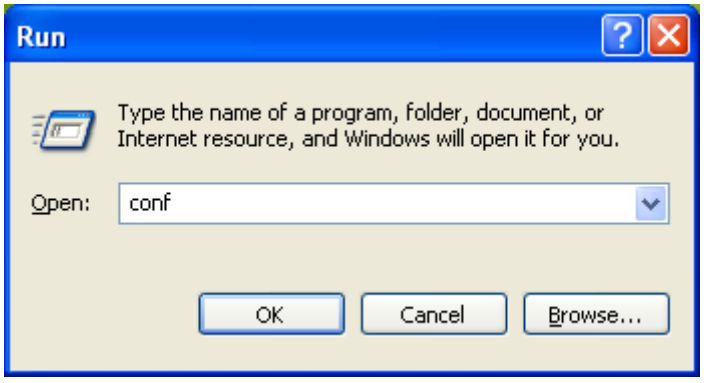
۲- در این حالت پنجره ای مانند روبرو نمایان می شود که دارای دو زبانه General و Support می باشد، زبانه دوم (Support) را انتخاب کنید. عبارت IP Address شماره IP سیستم شما را اعلام می کند.



۳- راه دیگر نیز این است که در محیط Command Prompt دستور IpConfig را وارد نمایید.

۱۳-۲- اجرا و پیکربندی نرم افزار

حال نوبت به آموزش نرم افزار می رسد. برای اجرای برنامه، ابتدا وارد Run شده و سپس دستور Conf را اجرا نمایید:



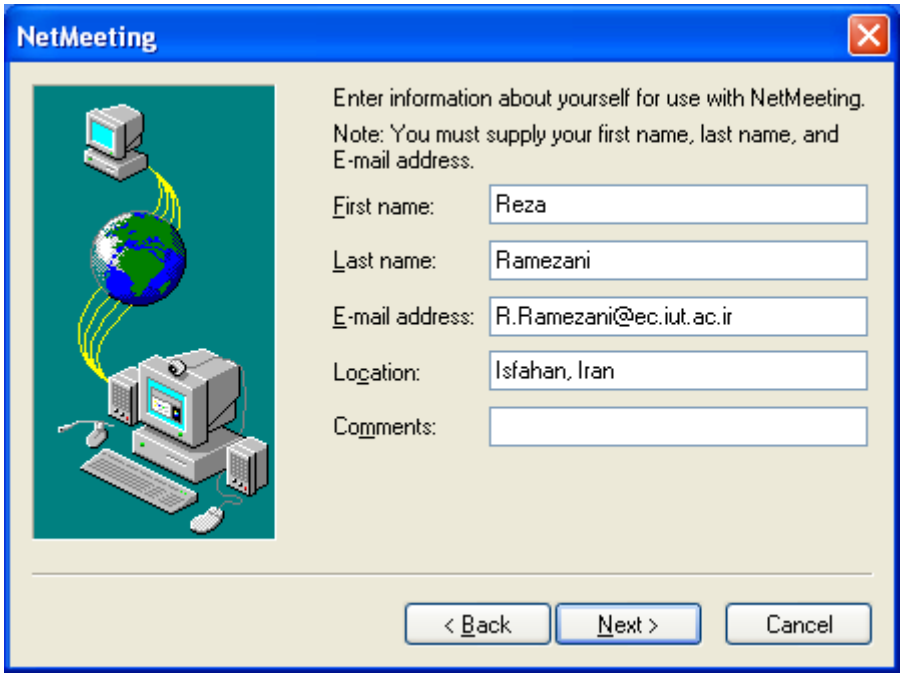
راه دیگر نیز اجرای مستقیم نرم افزار از طریق منوی Start است.

بعد از اجرا شدن صفحه زیر به ترتیب تا آخر NEXT را میزنیم.

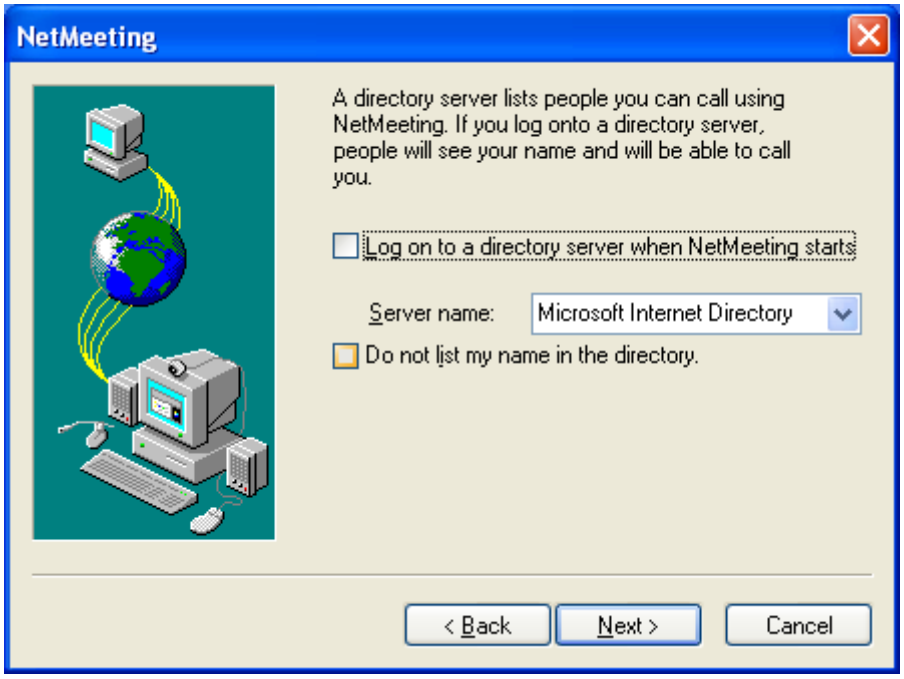
در قسمت زیر همانطور که می بینید، این قسمتها حتما باید پر شوند.

۱. **First Name**
۲. **Last Name**
۳. **Email Address**

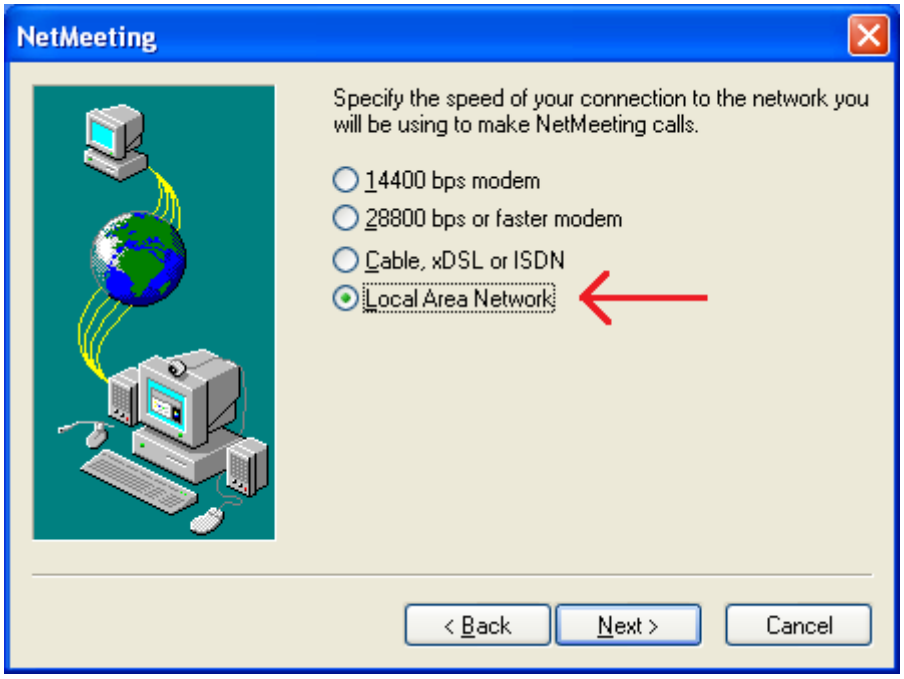
بقیه قسمت ها زیاد پر کردنش مهم نیست و ایمیل را هم می توانید یک مقدار فرضی وارد کنید و الزامی ندارد که حتما ایمیل خودتان باشد.



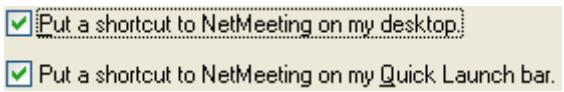
صفحه بعد امکان اتصال به Directory Server را به ما می دهد. بدون انتخاب آن، روی دکمه Next کلیک کنید.



چون در محیط شبکه محلی از این نرم افزار استفاده می کنید، گزینه آخر را انتخاب کرده و روی Next کلیک کنید.



در صفحه بعد می توانید محل قرار گیری میانبر های نرم افزار را تعیین نمایید. روی Next کلیک کنید.

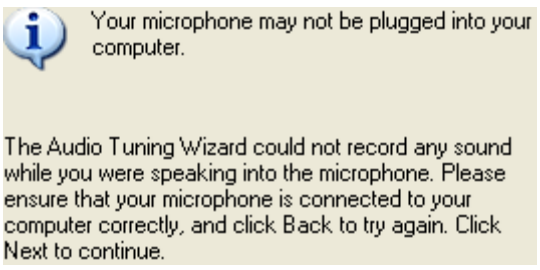


صفحه بعد، صفحه آغاز ویزارد میکروفون و اسپیکر می باشد. روی Next کلیک کنید.

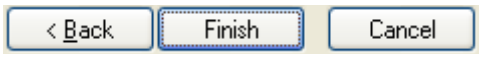
در صفحه جدید، با زدن دکمه Test، صدا را تست کرده و روی Next کلیک کنید.

این صفحه مربوط به تست ضبط صدا می باشد. روی Next کلیک کنید.

این صفحه وضعیت میکروفون را نشان می دهد. روی Next کلیک کنید.



در نهایت روی Finish کلیک کنید.



کار تمام شده و برنامه اجرا می شود.

۱۳-۳- نحوه کار با برنامه

در شکل زیر، صفحه اصلی برنامه را مشاهده می نمایید.

قسمت های مختلف برنامه به صورت زیر است:

A: Place Call، برای متصل شدن به کامپیوتر های محیط شبکه

B: End Call، برای خارج شدن و قطع اتصال برنامه از شبکه

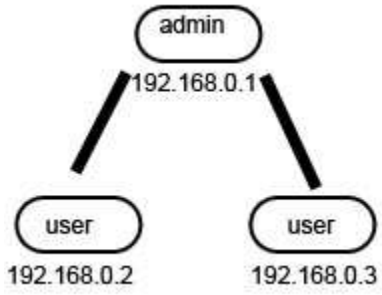
C: Transfer File، برای اشتراک گذاری و انتقال فایلها

D: White Board، برای نقاشی و.... (قابل مشاهده برای دیگران)

E: Chat، برای گفتمان و چت در محیط شبکه

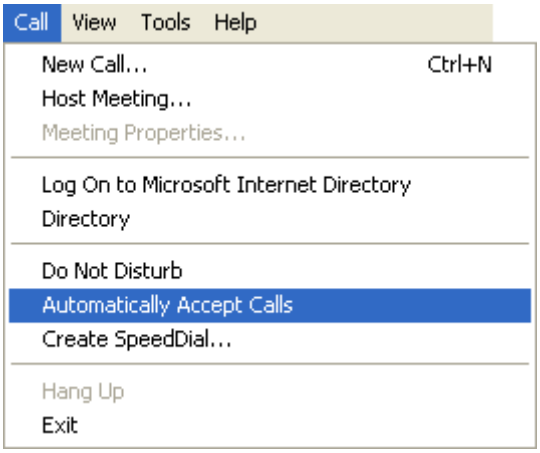
F: Share Program، به اشتراک گذاری برنامه ها برای دیگر کاربران

ما در محیط شبکه برای اتصال با برنامه NetMeeting به دیگر کامپیوتر ها، نیاز به IP داریم. هر کامپیوتر یک IP مخصوص به خود را دارد. مثلاً به صورت زیر:



فرض می کنیم که ما کامپیوتر شماره ۱ هستیم با آدرس ۱۹۲.۱۶۸.۰.۱ و می خواهیم به کامپیوتر شماره ۲ با آدرس ۱۹۲.۱۶۸.۰.۲ وصل بشویم. طبق شکل زیر عمل می کنیم. ابتدا آدرس IP کامپیوتر مقصد را وارد کرده و سپس روی دکمه Call کلیک می نماییم.

در این حالت، هر بار و هنگام اتصال از Client به Server، سیستم سوالی از کاربر Server منوط به پذیرش کاربر Client می پرسد. برای حذف این سوال، در برنامه اجرا شده در Server، از منوی Call گزینه Automatically Accept calls را انتخاب نمایید.



در کامپیوتری که قصد دارید تصویر آن را به اشتراک بگذارید، بر روی آیکون Share Program کلیک نمایید.

نکته: بعد از برقراری ارتباط NetMeeting موجود در سیستم ها با یکدیگر، انتخاب یکی از کامپیوتر ها برای Share تصویر، اختیاری بوده و لزومی ندارد دقیقاً کامپیوتر اصلی (مرکزی) را برای اشتراک تصویر در نظر بگیریم.

در کادر ظاهر شده عبارت Desktop را در سمت چپ و دکمه Share را در سمت راست انتخاب نمایید.

انتخاب عبارات دیگر (برنامه های در حال اجرا) موجب به اشتراک گذاشته شدن تصویر آن برنامه ها بر روی مانیتور سایر سیستم ها خواهد شد. در حالی که انتخاب کلمه Desktop کل محتویات صفحه نمایش شما را به اشتراک می گذارد.

بدین ترتیب تصویر کامپیوتر مورد نظر بر روی صفحه نمایش سایر کامپیوتر ها مشاهده خواهد شد. البته سیستم های دیگر، این تصویر را در ابعاد کوچکتر خواهند دید که برای بزرگ کردن اندازه آن می توان از کلیدهای ترکیبی CTRL+Enter یا ALT+Enter استفاده نمود.

جهت برداشتن Share تصویر نیز مجددا دکمه Share Program را فشرده، در کادر ظاهر شده، گزینه مورد نظر (Desktop) را انتخاب و دکمه Unshare یا Unshare All را کلیک می نماییم.

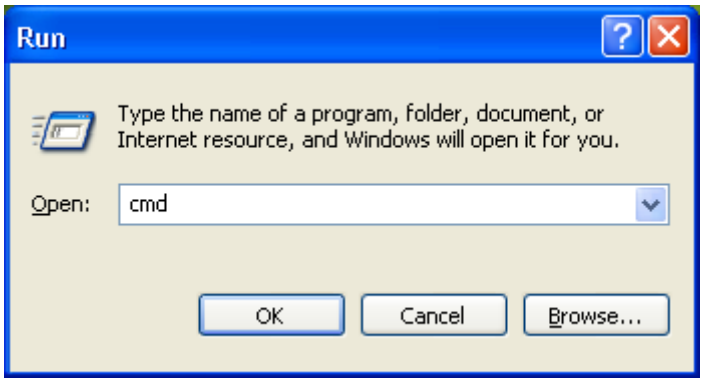
لازم به ذکر است بسته شدن نرم افزار NetMeeting موجب قطع ارتباط سیستم فعلی با سایر سیستم ها خواهد شد.

فصل ۱۴

دستورات پر کاربرد شبکه

۱۴-۱- محل اجرای دستورات

در این فصل به معرفی برخی دستورات شبکه می پردازیم. برای اجرای این دستورات بایستی از محیط Command Prompt استفاده نمایید. برای این کار وارد Run شده و تایپ کنید cmd.



۱۴-۲- دستور IPConfig

ipconfig، یکی از دستورات مفید به منظور بررسی وضعیت پیکربندی TCP/IP در کامپیوتر های سرویس دهنده و 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. در سیستم هایی که بر روی آنان ویندوز x۹ و یا ME نصب شده است، می توان از دستور winipcfg استفاده نمود.

استفاده از ipconfig

برای استفاده از دستور فوق، کافی است نام آن را از طریق پنجره command prompt تایپ نمود. عملکرد ipconfig و اطلاعاتی که در اثر اجرای آن نمایش داده خواهد شد به نوع سوئیچ استفاده شده، بستگی دارد.

استفاده از ipconfig بدون سوئیچ، اطلاعات پیکربندی TCP/IP در ارتباط با هر یک از آداپتورهای موجود بر روی سیستم را نمایش خواهد داد:

- **آدرس IP**
- **Subnet Mask**
- **Default Gateway**
- **اطلاعات سرویس دهنده DNS**
- **Domain**

تایپ دستور	خروجی
C:\> ipconfig	**Ethernet adapter MyLan1:** Connection-specific DNS Suffix.: IP Address..... : 10.10.1.1 Subnet Mask.....: 255.0.0.0 Default Gateway.....: **PPP adapter My ISP:** Connection-specific DNS Suffix.: IP Address..... : 10.1.1.216 Subnet Mask.....: 255.255.255.255 Default Gateway.....: 10.1.1.216

دستور فوق، اطلاعات مربوط به اتصالات از نوع PPP که از آنان 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 (آدرس MAC)
- اطلاعات مربوط به DHCP

تایپ دستور	خروجی
C:\> ipconfig /all	**Windows 2000 IP Configuration** Host Name.....: srco Primary DNS Suffix.....: srco. ir Node Type.....: Broadcast IP Routing Enabled.....: No WINS Proxy Enabled.....: No DNS Suffix Search List.....: srco. ir **Ethernet adapter MyLan1:** Connection-specific DNS Suffix.: Description.....: D-Link DFE-680TX CardBus PC Card **Physical Address.....: 00-50-BA-79-DB-6A** **DHCP Enabled.....: No** IP Address..... : 10.10.1.1 Subnet Mask..... : 255.0.0.0 Default Gateway.....: DNS Servers..... : 127.0.0.1 **PPP adapter My ISP:** Connection-specific DNS Suffix.: Description..... : WAN (PPP/SLIP) Interface Physical Address.....: 00-53-45-00-00-00 00-53-45-00-00-00

	DHCP Enabled.....: No IP Address..... : 10.1.1.216 Subnet Mask.....: 255.255.255.255 Default Gateway.....: 10.1.1.216 DNS Servers.....: x1.y1.z1. w1 x2.y2.z2. w2

سایر سوئیچ های دستور ipconfig: با استفاده از دستور ipconfig و برخی سوئیچ های آن (release، renew)، می توان 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 (در مورد DHCP در فصل های آینده صحبت خواهیم کرد). فرآیند فوق به منظور تشخیص عملکرد صحیح سرویس دهنده DHCP در شبکه بسیار مفید و سرور است. (آیا سرویس دهنده DHCP وظایف خود را به خوبی انجام می دهد؟ آیا یک سرویس گیرنده قادر به برقراری ارتباط با سرویس دهنده DHCP به منظور درخواست و دریافت اطلاعات پیکربندی TCP/IP می باشد؟). دستور ipconfig دارای سوئیچ های مفید متعددی است که می توان با توجه به نوع خواسته خود از آنان استفاده نمود:

سوئیچ	عملکرد
/ release [adapter]	آدرس IP پیکربندی شده توسط DHCP را آزاد می نماید. در صورتی که سوئیچ فوق را به تنهایی و بدون مشخص نمودن adapter تایپ نماییم، پیکربندی IP برای تمامی آداپتورهای موجود بر روی کامپیوتر، آزاد می گردد. در صورتی که قصد آزاد سازی اطلاعات پیکربندی مربوط به یک آداپتور خاص را داشته باشیم، می بایست به همراه سوئیچ فوق نام آداپتور نیز مشخص گردد. (مثلاً ipconfig / release MyLan1)
/ renew [adapter]	یک آدرس IP را بر اساس اطلاعات جدیدی که از طریق DHCP دریافت می نماید، پیکربندی مجدد می نماید. در صورتی که سوئیچ فوق را به تنهایی و بدون مشخص نمودن adapter تایپ نماییم، پیکربندی IP تمامی آداپتورهای موجود بر روی 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. (مثلاً ipconfig / renew MyLan1)
/flushdn	حذف محتویات Dns Resolver Cache
/registerdn	Refresh نمودن تمامی اطلاعات تولید شده توسط DHCP برای آداپتور و ریجستر 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 می توان با کلیک (Right click) بر روی Network Neighborhood و انتخاب گزینه Properties، از طریق پنجره Network and Dial-up Connections مشاهده نمود (اسامی آدپتور ها، نام آیکون ها می باشند).

مفهوم DNS Cache: زمانی که یک سیستم، ترجمه (تبدیل نام Host به آدرس) را از طریق یک سرویس دهنده DNS دریافت می نماید، برای مدت زمان کوتاهی آن را در یک Cache ذخیره می نماید. در صورتی که مجددا" از نام استفاده شود،

پشته TCP/IP محتویات Cache را به منظور یافتن رکورد درخواستی بررسی می نماید. بدین ترتیب امکان پاسخگوئی سریعتر به درخواست ترجمه نسبت به حالتی که در خواست برای یک سرویس دهنده DNS ارسال می شود، فراهم می گردد. با توجه به این که اندازه Cache نمی تواند از یک میزان منطقی و تعریف شده تجاوز نماید، هر رکورد موجود در Cache پس از مدت زمانی خاص حذف می گردد. در صورت اعمال هرگونه تغییرات در DNS (مثلاً تغییر یک رکورد DNS)، می توان با استفاده از دستور ipconfig/flushdns تمامی رکورد های موجود در Cache را حذف نمود. بدین ترتیب در صورت درخواست یک نام Host، با سرویس دهنده DNS مشورت می گردد و نتایج مجددا" در Cache ذخیره خواهند شد. دستور ipconfig /displaydns، محتویات Cache را نمایش خواهد داد. از اطلاعاتی که نمایش داده می شود، می توان به منظور تشخیص این موضوع که آیا برای ترجمه نام به آدرس از Cache و یا سرویس دهنده DNS استفاده شده است، کمک گرفت.

موارد استفاده از دستور Ipconfig: از دستور فوق در مواردی که قصد تشخیص این موضوع را داریم که آیا سرویس دهنده DNS و DHCP در شبکه به درستی وظایف خود را انجام می دهند، استفاده می شود(علاوه بر مشاهده اطلاعات پیکربندی TCP/IP). مثلاً با استفاده از سوئیچ های release و renew، می توان براحتی تشخیص داد که آیا در زمینه دریافت اطلاعات پیکربندی از یک سرویس دهنده DHCP مشکل خاصی وجود دارد. از سوئیچ های مرتبط با DNS می توان به منظور اعمال تغییرات پیکربندی، بهنگام سازی cache محلی و یا رجیستر نمودن اطلاعات پیکربندی جدید با یک سرویس دهنده DNS، استفاده نمود.

۱۴-۳- دستور Ping

Ping دستوری است که مشخص می کند که آیا یک کامپیوتر خاص که ما IP یا Hostname (نام کامپیوتر) آن را می دانیم، روشن و فعال (Active) 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.

استفاده از این دستور به صورت زیر است:

Ping [IP-or-Hostname]

که به جای IP-or-Hostname باید آدرس IP و یا Hostname کامپیوتر مورد نظر را بگذاریم.

مثلاً Ping iut.ac.ir (سایت دانشگاه صنعتی اصفهان) را در command prompt تایپ کردم و به نتایج زیر رسیدم :

```
Pinging iut.ac.ir [217.219.19.121] with 32 bytes of data:
Reply from 217.219.19.121: bytes=32 time=1402ms TTL=105
Reply from 217.219.19.121: bytes=32 time=941ms TTL=105
Reply from 217.219.19.121: bytes=32 time=981ms TTL=105
Reply from 217.219.19.121: bytes=32 time=851ms TTL=105
Ping statistics for 217.219.19.121:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
Minimum = 851ms, Maximum = 1402 ms, Average = 1043ms
```

این نتایج نشان می دهد که iut.ac.ir فعال است.

در نتیجه 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 گام های اعتبار بسته ارسالی است.

حالا به کامپیوتری با آدرس IP شماره ۲۱۷.۲۱۹.۱۹.۱۲۱ (که همان iut.ac.ir است)، Ping می کنیم. نتایج همان است فقط با تغییراتی در سطر اول. (البته time که معنای مدت زمان رسیدن بسته را می دهد، با توجه به ترافیک شبکه، کم و زیاد خواهد شد). برای Ping کردن به این IP، دستور Ping ۲۱۷.۲۱۹.۱۹.۱۲۱ را صادر می کنیم.

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

Pinging 217. 66.196.1 with 32 bytes of data :

Request timed out .

Request timed out .

Request timed out .

Request timed out .

Ping statistics for 217. 66.196.1:

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 تمام مطالبی که در بالا ذکر شد، در حالتی است که مستقیماً به اینترنت وصل شده اید و یا اگر از طریق شبکه محلی به اینترنت وصل هستید، شبکه شما به درستی پیکربندی 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 **interrupted** شدن توسط کاربر به Ping کردن ادامه دهد. یعنی کار ارسال بسته تا بینهایت ادامه یابد، مگر اینکه کاربر آن را متوقف کند.

۲) Ping –a

با استفاده از پارامتر **"a"** نیز میتوان نام هاست IP مورد نظر را پیدا کرد. به عبارتی این پارامتر نام هاست متناظر با IP را نمایش میدهد.

۳) Ping –n

با استفاده از پارامتر **"n"** نیز میتوان تعداد دفعات ارسال **Echo Request messages** را که به طور پیش فرض **چهار بار** میباشد 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** میباشد تغییر داد. بیشترین مقدار مجاز برای این پارامتر **۶۵,۵۲۷** میباشد.

۵) Ping –i

با استفاده از پارامتر **"i"** نیز میتوان مدت زمان زنده بودن بسته 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 ای پی **Echo Request messages** را تعیین کرد. مقدار پیش فرض ۰ میباشد. محدوده مجاز این مقدار نیز ۰ تا ۲۵۵ می باشد.

۷) Ping -w

با استفاده از پارامتر **"w"** نیز میتوان مدت زمان انتظار برای دریافت پاسخ از هاست بر حسب milliseconds را تعیین نمود.

۱۴-۴- دستور Tracert/Traceroute

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 ارسالی ما برای رسیدن از مبدا به مقصد از چه دستگاه هایی عبور می کند. این دستور از طریق پروتکل ICMP این عمل را انجام می دهد و آن بدین صورت است که بسته Echo Request توسط کامپیوتر ما به دستگاه مقصد ارسال می شود و در هر مرحله ای از این مسیر، بسته Echo Reply ایجاد شده و به کامپیوتر مبدا (کامپیوتر ما) ارسال می شود. باید این نکته را خاطرنشان کنم هریک از چهار سیستم عامل معروف امروزی دارای دستور ویژه خود در این ابزار هستند که در زیر لیست آن ها را آورده ایم:

Windows Server 2000/2003 tracert
Novell NetWare iptrace
Linux/UNIX/ Macintosh traceroute

این دستور علاوه بر اینکه اطلاعات جامعی از هر یک از مسیر یاب های مسیر تا رسیدن به مقصد به ما می دهد بلکه نام آن مسیر یاب ها را در صورتی که در آن ها تنظیم شده و در دسترس قرار گرفته باشد نشان خواهد داد. همچنین زمان رفت و برگشت بسته ICMP ما از مبدا تا مسیر یاب بین راه، بر مبنای 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. در زیر یک نمونه موفق از استفاده از این دستور در ویندوز ۲۰۰۳ را مشاهده می کنید:

C:\>tracert 24.7.70.37

Tracing route to c1-p4.sttlwa1.home.net [24.7.70.37] Over a maximum of 30 hops:

1 30 ms 20 ms 20 ms 24.67.184.1
2 20 ms 20 ms 30 ms rd1ht-ge3-0.ok.shawcable.net [24.67.224.7]
3 50 ms 30 ms 30 ms rc1wh-atm0-2-1.vc.shawcable.net [204.209.214.193]
4 50 ms 30 ms 30 ms rc2wh-pos15-0.vc.shawcable.net [204.209.214.90]
5 30 ms 40 ms 30 ms rc2wt-pos2-0.wa.shawcable.net [66.163.76.37]
6 30 ms 40 ms 30 ms c1-pos6-3.sttlwa1.home.net [24.7.70.37]

Trace complete.

درست مانند سایر دستورات که در این بخش با آن پرداخته ام دستور tracert هم دارای ستون هایی است که اطلاعات مورد نیاز ما در آن تفکیک شده اند. ستون اول شماره هاپ (گام های طی شده) را مشخص کرده است؛ به روایت دیگر یعنی جایی که بسته ICMP ارسالی کامپیوتر ما با آن رسیده است. سه ستون دیگر نمایانگر زمان ارسال و برگشت بسته ارسالی به میلی ثانیه و آخرین ستون نام Host مقصد و آدرس IP دستگاه پاسخ دهنده را مشخص می کند. بدیهی است درصورت وجود مشکل در مسیر ارتباطی به مقصد Trace route های ما موفقیت آمیز نخواهند بود. در مثال زیر نمونه ای از آن را مشاهده می کنید:

C:\>tracert comptia.org

Tracing route to comptia.org [216.119.103.72]

Over a maximum of 30 hops:

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.
9 * * * Request timed out.
10 * * * Request timed out.

در این مثال بسته ارسالی ICMP ما تنها موفق شده تا هفت مرحله پیش برود و در مرحله هشتم به مشکل برخورد کرده است که دلیل آن می تواند این باشد که دستگاهی که در مرحله هشتم قراردارد قطع است و یا اینکه دستگاه موجود در مرحله هفتم کار می کند. اما امکان مشخص کردن هاپ بعدی را ندارد. عوامل بسیاری می تواند وجود داشته باشد که دستگاه مرحله هفت قادر به انجام وظیفه نگردیده است که ممکن است مشکل در جدول Route آن باشد و یا Connection صحیحی برای آنان ایجاد نشده باشد. با توجه به موارد بالا متوجه می شوید که توسط این دستور شما بررسی مشکل را تنها بر روی یک یا دو دستگاه محدود کرده اید. این دستور همچنین می تواند به شما کمک کند تا شبکه های در مسیر با بار زیاد و متراکم را محدود سازید.

۱۴-۵- دستور NetStat

NetStat مخفف Network Statistics، یک ابزار خط فرمان است که اتصالات شبکه را (هم به داخل و هم به خارج)، 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 گر حجم اطلاعات رد و بدل شده در شبکه به عنوان یک اندازه گیر عملکرد استفاده می شود.

پارامترهای ورودی

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

بدون پارامتر: نمایش Connection های فعال

a– : نمایش تمامی اتصالات TCP و UDP فعال در کامپیوتر.

b– : نمایش برنامه درگیر با اتصالات شبکه ای نمایش داده شده در لیست خروجی. (در ویندوز ۲۰۰۰ و ویندوز های قبل از آن و سایر سیستم عامل های غیر ویندوزی امکان پذیر نیست)

e– : نمایش آمار مربوط به اترنت، از قبیل تعداد بایت ها و بسته های دریافتی و ارسالی. این پارامتر می تواند با s- نیز ترکیب شود.

f– : نمایش FQDN برای آدرس های خارجی. (فقط در ویندوز Vista و سیستم عامل های جدیدتر)

g– : نمایش کارت های شبکه و آمار آن ها. (در ویندوز موجود نیست، ipconfig می تواند این کار را در ویندوز انجام دهد)

n– : نمایش ارتباط های TCP فعال، هر چند که IPها و پورت ها را به صورت عددی نمایش می دهد و تلاشی برای تشخیص نام آن ها نمی کند.

m– : نمایش آمار مربوط به استریم ها.

o– : نمایش اتصال های TCP فعال به همراه PID مربوط به آن اتصال.

p– : در ویندوز، پروتکل مربوط به اتصال را نمایش می دهد. (TCP، UDP، ICMP، IP، ...)

p– : در لینوکس فرآیندهای مربوط به اتصال را نشان می دهد. (مانند کلید b- در ویندوز عمل می کند) (برای اجرای صحیح دستور باید دسترسی پایه یا root داشت.)

P– : در سولاریس، پروتکل مربوط به اتصال را نمایش می دهد. (TCP، UDP، ICMP، IP، ...)

r– : جدول هدایت IPها را نشان می دهد. (معادل دستور **route print** در ویندوز است.)

s– : نمایش آمار به تفکیک پروتکل.

v– : وقتی که با b- استفاده شود، توالی اجزای برنامه ها را نشان می دهد.

h– یا help-- : نمایش راهنمایی برای دستورات موجود. (مناسب برای سیستم های شبه یونیکس)

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

۱۴-۶- دستور Net

دستور Net بیشتر برای کار با Objectهای شبکه ای مورد استفاده قرار می گیرد. با این دستور بایستی کلمه ای دیگر مثل User یا Computer وارد کنید تا سیستم متوجه بشود که می خواهید با چه نوع Objectی کار کنید.

نام دستور	شرح دستور
Net Accounts	با این دستور، وضعیت تنظیمات پسوردها (مثل طول عمر) نشان داده می شود.
Net Computer	کامپیوتر ها را به پایگاه داده ی Domain مورد نظر اضافه و یا کم می کند.
Net Continue	سرویسی که توسط دستور Net Pause معلق شده است را دوباره راه اندازی می کند.
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 می شود فهمید در هر کدام از این گروه ها چه حساب هایی وجود دارد و نیز می شود به یک گروه خاص حسابی اضافه کرد. می خواهیم ببینیم که چه گروه های محلی تعریف شده است. می نویسیم: Net localgroup که نتیجه می شود: Aliases for \\Computer-name *Administrators Backup Operators Debugger Users *DHCP Administrators DHCP Users Guests *Power Users Replicator Users The command completed successfully. دقت کنید که ویندوز معمولاً هنگام ارائه نتایج دستورات Net، می آید و اول اسم هر گروه یک * قرار می دهد تا با حساب ها اشتباه نشود. حالا می خواهیم ببینیم که مثلاً در گروه Administrators چه حساب هایی هست. می نویسیم: Net localgroup Administrators که نتیجه می شود: Alias nameAdministrators Comment Administrators have complete and unrestricted accessto thecomputer/Domain Members Administrator Ali Reza The command completed successfully. پس سه تا حساب در حد Admin داریم. حالا می خواهیم مثلاً حساب Ali را از لیست Admin ها خارج کنیم، می نویسیم: Net localgroup Administrators Ali /delete و با این کار حساب Ali از گروه حذف می شود (می توانید دوباره لیست بگیرید و ببینید که کاربر Ali دیگر در این گروه نیست). حالا می خواهیم دوباره حساب Ali را به این گروه اضافه کنیم، می نویسیم: Net localgroup Administrators Ali /add این دستور از جمله مهم ترین دستوراتی است که باید یاد بگیرید. گاهی با حسابی وارد می شویم و می

	خواهیم که این حساب را به حد Admin برسانیم و روش کار همین دستور آخری است (اینکه اجازه این کار را داریم یا نه، بحثی است که در این مبحث نمی گنجد). وقتی حسابی وارد گروه Admin می شود، تمام مزایای این گروه را به دست می آورد.
Net Help	این دستور در واقع Help دستور Net است.
Net Helpmsg	وقتی که یک دستور Net به صورتی اجرا می شود که خطایی پیش بیاید، ویندوز یک شماره خطای ۴ رقمی به ما می دهد که برای دریافت جزئیات بیشتر در مورد این خطا باید از دستور Net helpmsg استفاده کنیم.
Net Localgroup	گروهای محلی را نمایش، اصلاح یا اضافه می کند.
Net Name	این دستور به یک پیام نام اختصاص می دهد و یا نام آن را پاک می کند.
Net Pause	سرویس های درحال اجرا را متوقف می کند.
Net Print	اطلاعات مربوط به یک صف مشخص را نمایش می دهد؛ اطلاعات مربوط به تمامی صف های مربوط به سرور نوشته شده را نمایش می دهد؛ اطلاعات مربوط به یک کار مشخص را نشان می دهد و یا کار مشخص شده را کنترل می کند.
Net Send	فرض کنید که می خواهیم یک Message به فرد خاصی که به سیستم وارد شده است و یک Session دارد بفرستیم (اینکه فردی Session دارد یا نه، به کمک دستور Net Session قابل بررسی است). بدین منظور از این دستور می توانیم استفاده کنیم. مثلاً اگر بخواهیم به Administrator که الآن در سیستم هست، پیغام Salam Mashti را بفرستیم، می نویسیم: Net Send Administrator Salam Mashti در این حالت کاربر Administrator، پیغام ما را می گیرد. اگر بخواهیم به همه افرادی که الآن Session دارند، همین پیغام را بفرستیم، می نویسیم: Net Send /Users Salam Mashti و پیغام را همه می گیرند. این دستور باید به صورت Local یعنی از طریق یک Shell اجرا شود.
Net Session	به کمک این دستور مشخص می شود که چه کسانی الآن در سیستم یک Session دارند. به عبارت دیگر، برای مشاهده اینکه چه کسانی به صورت Remote به سیستم وارد شده اند. این دستور را تایپ کنید: Net Session تا لیست این افراد نمایان شود. اگر بخواهیم همه Session ها را خاتمه بدهیم، می نویسیم: Net Session /delete این دستور، رابطه این کامپیوتر با سایر کامپیوترهای شبکه قطع می کند (نه ارتباط فیزیکی، بلکه اتصالاتی که مثلاً با برنامه Remote Desktop ایجاد شده اند). اگر فقط بخواهیم یک Session را با یک کامپیوتر خاص تمام کنیم، می نویسیم: Net Session \\xxx.xxx.xxx.xxx /delete این در حالتی است که با آن کامپیوتر Session داشته باشم. دقت کنید که به جای دستور Net Session می توانید از دستور Net Sessions یا Net Sess استفاده کنید.
Net Share	این دستور به ما کمک می کند که Share ها را به صورت محلی مدیریت کنیم (دستور بالایی به صورت Remote استفاده می شود). می خواهیم ببینیم که الآن چه Share هایی وجود دارد. می نویسیم: Net Share

	و جواب می گیریم: Share name ResourceRemark
Net Start	سرویس های شبکه را آغاز یا لیست می کند.
Net Statistics	آمار مربوط به پایگاههای کاری یا سرور ها را نشان می دهد.
Net Stop	سرویس ها را متوقف می کند
Net Time	ما از این دستور برای فهمیدن زمان روی یک سرور استفاده می کنیم. اگر به صورت محلی استفاده می کنید، بنویسید: Net Time ولی اگر به صورت Remote، می خواهید زمان یک کامپیوتر را پیدا کنید، بنویسید: Net time \\xxx.xxx.xxx.xxx که xxx.xxx.xxx.xxx همان آدرس IP است که برای آن Session داریم.
Net Use	این دستور دو کاربرد مهم دارد. اولین کاربرد، Connect یا Disconnect شدن به یک کامپیوتر با پورت ۱۳۹ باز (یعنی Firewall آن پورت را نبسته باشد) و NetBIOS فعال است. مثلاً اگر بخواهیم با حساب Administrator و با پسورد ۱۲۳ به کامپیوتری با آدرس IPای xxx.xxx.xxx.xxx متصل شده و به پوشه Share شده ای به اسم IPC$ دسترسی یابیم، (این Share معمولاً هست، به همین دلیل از این Share استفاده کردیم)، می نویسیم: Net use \\xxx.xxx.xxx.xxx\IPC$ "123" /User:"Administrator" این کاربرد اول بود که این را قبل از دستور Net view انجام می دهیم. می توانستیم یک null Session تشکیل دهیم، به این صورت که قسمت مربوط به Username و Password را خالی بذاریم. به این صورت: Net use \\xxx.xxx.xxx.xxx\IPC$ "" /User: "" حالا Session تشکیل شده است. کاربرد بعدی اینه که بعد از اینکه دستور بالا را اجرا کردیم و بعد دستور Net view را اجرا کردیم و لیست کامل Share ها را بدست آوردیم، بیاییم و یکی از این Share ها را استفاده کنیم. مثلاً اگر اسم Share که لیست شده، SharedDocs باشد، و بخواهیم یک درایو جدید (Map Drive) را به آن نسبت بدهیم که بتوانیم با آن کار کنیم، می نویسیم: Net use * \\xxx.xxx.xxx.xxx\SharedDocs معنی کاراکتر * این است که اگر مثلاً آخرین درایو در کامپیوتر من (با احتساب سی-دی درایو) مثلاً G باشد، درایوی که برای اتصال به پوشه Share شده استفاده می شود، درایو بعدی یعنی H می باشد. می توانستیم اینطوری هم بنویسیم: Net use H: \\xxx.xxx.xxx.xxx\SharedDocs خوب حالا می توانیم مثل یک درایو محلی با آن پوشه Share شده کار کنیم. وقتی کارمان با Share تموم شد، باید Disconnect کنیم، با این دستور: Net use /delete H:
Net User	این دستور به ما کمک می کند که به صورت محلی بدانیم که چه حساب هایی در سیستم تعریف شده است و نیز اینکه اطلاعاتی در مورد هریک بدست آورده و نیز حساب جدید تعریف کنیم. اول می خواهیم بدانیم چه حساب هایی تعریف شده، می نویسیم: Net User

	که نتیجه می شود: User accounts for \\computer-name Administratorali Reza ASPNET Guest The command completed successfully. خوب حالا مثلاً می خواهیم راجع به حساب Reza اطلاعاتی بگیرم، می نویسیم: Net User Reza و جواب می گیریم: User name Guest User name Reza Full Name Comment User's comment Country code 000 (System Default) Account active 0es Account expires Never Password last set 24/11/2010 06:33:06 .â Password expires Never Password changeable 24/11/2010 06:33:06 .â Password required No User may change password Yes Workstations allowed All Logon script User profile Home directory Last logon 26/12/2010 07:54:48 Logon hours allowed All Local Group Memberships *Administrators *Debugger Users *HelpLibraryUpdaters *HomeUsers Global Group memberships *None The command completed successfully. می بینید که در سطر ۲ تا مانده به آخر (سطر Local Group Membership) دقیقا بیان شده است که این حساب به چه گروه هایی تعلق دارد. دقت کنید که به جای دستور Net User، از دستور Net Users هم می توانید استفاده کنید. حالا می خواهیم یک حساب جدید اضافه کنیم. اسم حساب می خواهیم Ali بوده و رمز عبور آن 123 باشد، می نویسیم: Net User Ali 123 /Add حالا می خواهیم همین حساب را پاک کنیم: Net User Ali /delete دقت کنید که در دستور پاک کردن دیگر لزومی به وارد کردن رمز عبور نیست.
Net View	فرض کنید که یک Netbios Session تشکیل داده ایم (یعنی به یک کامپیوتر ره دور متصل شده ایم؛ مثلاً توسط تایپ آدرس IP آن در Run) (گاهی Null Session هم جواب می دهد) و حالا می خواهیم ببینیم که چه منابعی برایمان Share شده است، می نویسیم: Net view \\xxx.xxx.xxx.xxx

و مثلاً جواب می گیریم: Shared resources at \\xxx.xxx.xxx.xxx Share name Type Used asComment SharedDocsDisk The command completed successfully. می بینید که SharedDocs، پوشه ای است که Share شده است. حالا با دستور Net use می تـوانیم از Share استفاده کنیم.	

۱۴-۷- دستور nslookup

nslookup.exe ابزاری است که به مدیران شبکه امکان تست و رفع اشکال سرویس DNS را می دهد. Nslookup یک برنامه از نوع خط فرمان (command-line) است که مخفف Name Server Lookup می باشد. بـه وسـیله NSLookup مـی تـوان از Name Serverهای مختلف اطلاعات مربوط به دامنه های مورد نظر را در صورت امکان بدست آورد. اطلاعاتی که درباره دامنه از طریق NSLookup مشاهده می کنیم، در واقع همان اطلاعاتی است که در ZoneFile مربوط به دامنه وجود دارد.

آشنایی کامل با امکانات این دستور برای یک مدیر شبکه که با سرویس DNS سروکار دارد خیلی مهم و حیاتی است.

nslookup را می توان به دو شکل **Interactive** و **غیر Interactive** استفاده کرد.

حالت **غیر Interactive** تنها زمانی کاربرد دارد که فقط قصد اجرای یک دستور را دارید و علاقه دارید پس از اتمام آن دوباره به محیط command برگردید.

شکل دستور nslookup در محیط **غیر Interactive** به صورت است:

nslookup [-option] [hostname] [server]

برای استفاده از nslookup به صورت **Interactive** کافی است دستور **nslookup** را وارد کنید.

پس از ورود به محیط دستور nslookup محیطی مانند شکل زیر نمایش داده می شود:

دستور nslookup پس اجرا شدن، با توجه با تنظیمات TCP/IP کامپیوتر شما، DNS پیش فرض کامپیوتر را به عنـوان سـرور انتخاب می کند و سعی می کند با استفاده از ارسال درخواست Reverse نام سرور را نیز پیدا کرده و به شما نمایش دهد.

اگر موفق به تبدیل IP به نام شود، در قسمت Default Server، نام سرور را نمایش می دهد در غیـر ایـن صـورت Unknown نمایش داده می شود، اینکه nslookup موفق با تبدیل IP به نام شود یا نه تاثیری بر دستوراتی کـه در ادامـه وارد مـی کنیـد ندارد و تنها برای اطلاع شما است.

در قسمت Address هم آدرس IP سرور را نمایش می دهد در خط بعد با نمایش علامت > منتظر دریافت دسـتور مـی شـود. حال شما می توانید دستورات دلخواه خود را وارد نمایید.

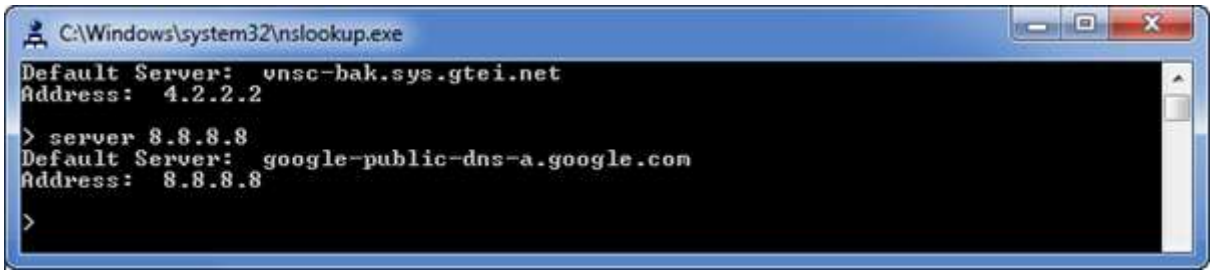
برای مشاهده لیست دستورات و توضیحات آنها می توانید از علامت ? یا دستور Help استفاده کنید.

برای خروج از nslookup نیز می توانید از کلید های Ctrl+C یا دستور Exit استفاده کنید.

اگر قصد تست کردن سرور دیگری غیر سرور مشخص شده در قسمت Address دارید می توانید از دستور زیر استفاده کنیـد. بدین ترتیب دستوراتی که در ادامه وارد می کنیم، به این سرور ارجاع داده می شود:

server <server ip/name>

مثال: برای اینکه سوالاتی که در آینده از nslookup می پرسیم به DNS سروری با آدرس ۸.۸.۸.۸ ارجاع شـود بایـد بـه ایـن صورت عمل کنید:



برای اینکه نوع رکوردی که می خواهید از DNS سرور پرسیده شود را تغییر دهید، باید بـه کمـک دسـتور Set Type یـا Set Querytype این کار را انجام دهید و مقدار Type را به یکی از موارد زیر تغییر دهید:

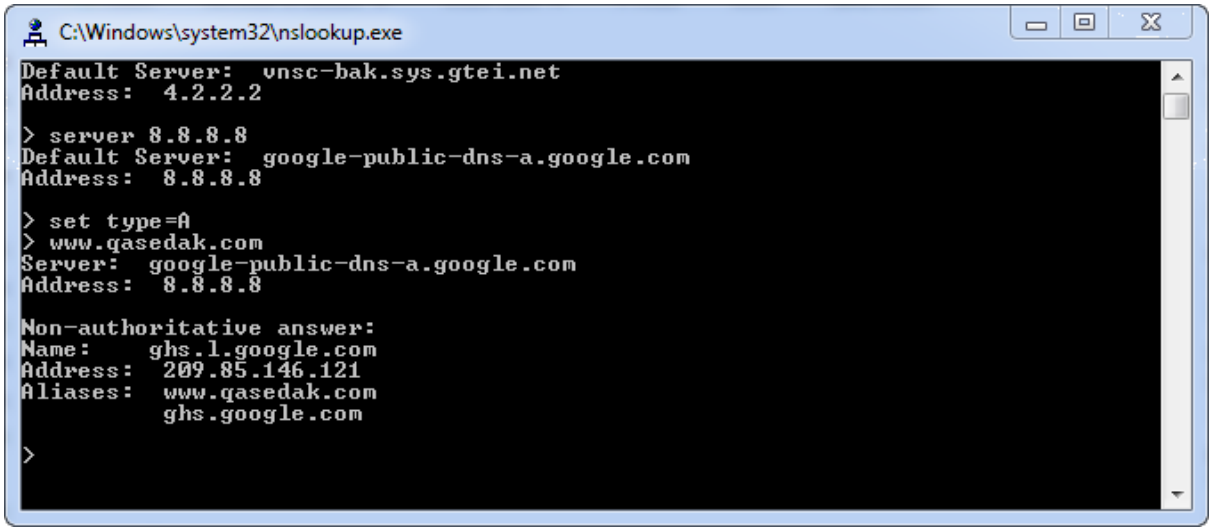
A, CNAME, MX, NS, PTR, SOA, SRV A, AAAA, A+AAAA, ANY

مفهوم این کلمات در فصل DNS Server آمده است.

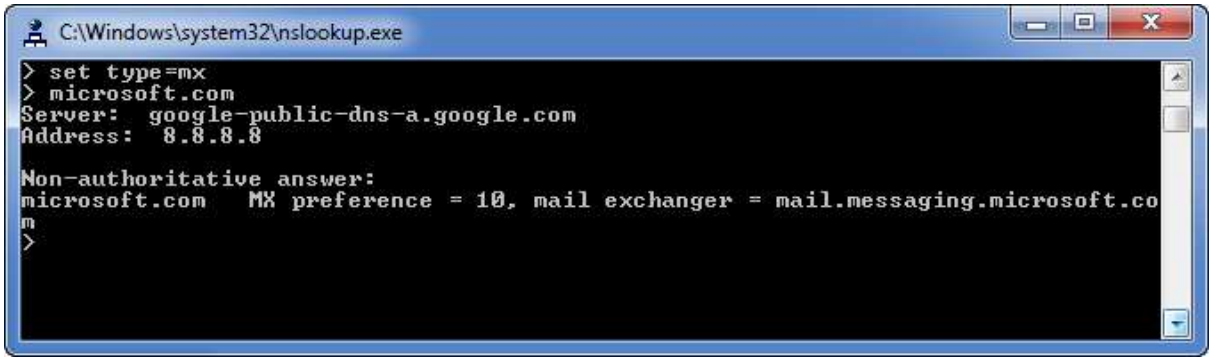
در صورتی که متغیر Type را مشخص نکنید، از حالت پیش فرض یعنی A+AAAA استفاده می شود.

پس از مشخص نمودن نوع سئوال می توانید درخواست خود را تایپ و کلید Enter را بزنید. بدین ترتیب پرس و جو های شما به پرس و جو های خاصی محدود می شود. مثلاً فقط IP کامپیوتر ها یا فقط Mail Server ها.

مثال (۱): برای تبدیل نام www.qasedak.com به IP



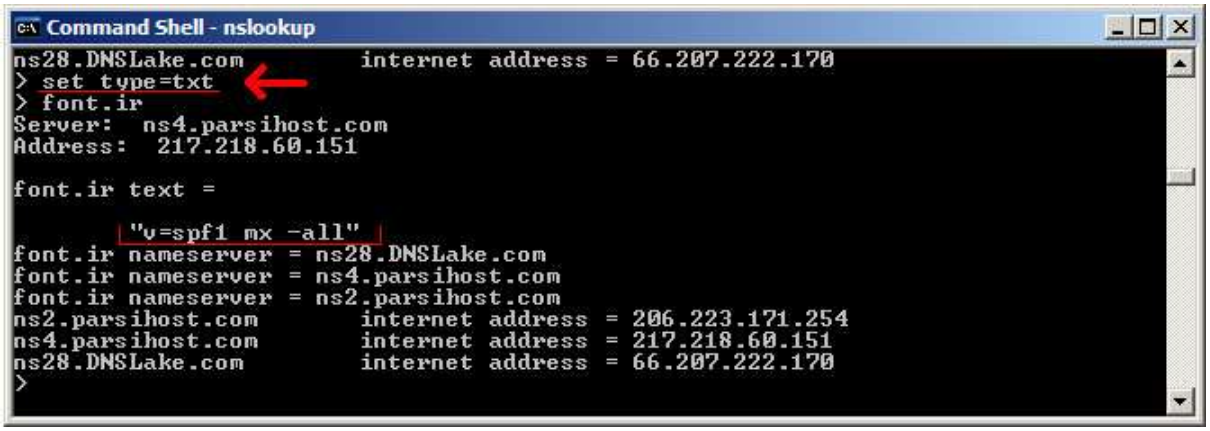
مثال (۲): برای اطلاع از Mail Serverهای موجود در دامنه Microsoft.com



نکته مهم: اگر nslookup در جواب، عبارت Non-authoritative answer را نمایش داد، به این معنی است که سـروری کـه از آن سوال شده، جواب را از Cache خوانده و به سراغ سرور مسئول دامنه نرفته و اگر این عبارت وجود نداشت یعنی اینکه سوال مستقیماً از سرور مسئول دامنه پرسیده شده است. معمولاً اگر در این حالت یک بار دیگر سئوال را تکرار کنیـد عبـارت Non-authoritative نمایش داده می شود.

مثال (۳): پرس و جوی رکوردهای TXT

دستور set type=txt را تایپ می کنیم و درباره دامنه font.ir پرس و جو می کنیم.



همانطور که در شکل می بینید، دستور فوق اطلاعات مربوط به رکورد TXT دامنه را نمایش می دهد.

دیگر امکانات دستور nslookup

۱) تست ZoneTransfer

برای اینکه عمل ZoneTransfer را توسط nslookup شبیه سازی کنید می توانید از دستور ls استفاده کنید. مثال: ls -d <zone name>

۲) Timeout

در صورت کندی اینترنت یا DNS سرور می توانید زمان Timeout را بالا ببرید. مقدار پیش فرض ۲ ثانیه است. مثال: set timout=<timeout second>

برای مشاهده تنظیمات فعلی nslookup، از دستور set all استفاده کنید.

۱۴-۸- دستور Whoami

دستور Whoami (Who am I?) نام دامنه، نام رایانه، نام کاربر و نام گروه هایی که کاربر عضو آن می باشد را نشان می دهد:

whoami [{/user | /groups | /priv} / all]

پارامتر ها:

User: برای نمایش نام کاربر به همراه نام دامنه

Groups: نام گروه هایی که کاربر عضو آن می باشد را نشان می دهد.

Priv: مجوز هایی که با کاربر داده شده است را نشان می دهد. مانند قابلیت تغییر ساعت ویندوز، نصب و حذف برنامه ها، تغییرات در تنظیمات شبکه و ...

All: تمامی موارد فوق.

۱۴-۹- دستور Getmac

این دستور برای نمایش آدرس فیزیکی کارت شبکه به همراه لیستی از پروتکل های شبکه ای که به کارت شبکه مربوط می شود، استفاده می شود. آدرس فیزیکی ۱۲ رقم طول دارد که کاراکتر ها بر مبنای هگزا دسیمال (مبنای ۱۶) می باشد که توسط خط تیزه از هم جدا می شوند. مثلاً به آدرس روبرو دقت نمایید: 00-15-18-00-04-F9. آدرس فیزیکی تجهیزات شبکه بوده و تکراری نیست. همچنین این آدرس ها قابلیت تغییر نیز ندارند. مثال:

```
C:\> GetMac
Physical Address        Transport Name
=================       ==========================================
08-00-27-0A-90-59       \Device\Tcpip_{F6ED027D-A0B6-49B9-84C5-2736E61146CA}
```

پارامتر ها:

/s: برای مشخص کردن نام رایانه یا آدرس IP

u/: برای مشخص کردن نام کاربر به همراه نام دامنه

p/: برای مشخص کردن کلمه عبور. معمولاً این پارامتر به همراه پارامتر u/ استفاده می شود و مورد آن زمانی است که بخواهیم آدرس فیزیکی یک رایانه راه دور را ببینیم. به همین دلیل باید نام کاربری و کلمه عبور رایانه راه دور را داشته باشیم.

۱۴-۱۰- دستور SFC

دستور SFC یا System File Checker نسخه و صحت کلیه پرونده های سیستمی ویندوز را از روی سی دی ویندوز بررسی می کند و اگر مغایرتی بین این پرونده ها پیدا کند، آن را مجددا از روی سی دی کپی کرده و آن را اصلاح می کند. قالب دستور به صورت زیر است:

Sfc [/scannow] [/scanboot]

پارامتر ها:

scannow/: این دستور تمامی پرونده هایی که توسط ویندوز محافظت می شود را بلافاصله اسکن و بررسی می نماید.

scanboot/: این دستور تمامی پرونده هایی که توسط ویندوز محافظت می شود را هر بار که رایانه راه اندازی می شود را اسکن و بررسی می نماید.

۱۴-۱۱- دستور SystemInfo

این دستور گزارش کاملی از کلیه تجهیزات سخت افزاری و سیستم عامل نشان می دهد.

فصل ۱۵

آموزش نصب ویندوز سرور ۲۰۰۳

برای نصب ویندوز ۲۰۰۳ چند مرحله پیش رو داریم:

۱۵-۱- ابتدا باید طرحی برای نصب داشته باشیم.

یعنی باید موارد زیر را در نظر بگیریم.

۱. موارد مورد نیاز سیستم را باید چک کنیم.
۲. باید سازگاری نرم افزار و سخت افزار را چک کنیم.
۳. باید نحوه پارتیشن بندی را چک کنیم.
۴. فایل سیستم مناسب را انتخاب کنیم.
۵. تصمیم گیری در مورد اینکه شبکه ما به صورت Workgroup باشد و یا Domain.
۶. تهیه چک لیست قبل از نصب برای چک کردن موارد بالا.

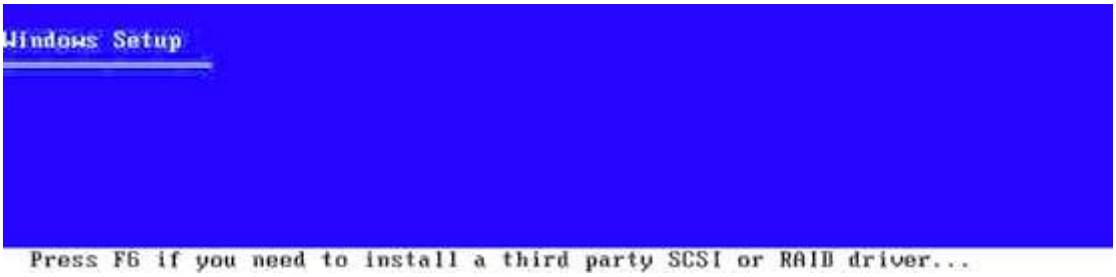
۱۵-۲- شروع عملیات نصب در مرحله متنی

راه های نصب متفاوتی برای نصب ویندوز ۲۰۰۳ وجود دارد؛ ولی مهم نیست که از کدام روش استفاده می شود چون تمام روشها تقریباً به یک گونه می باشد.

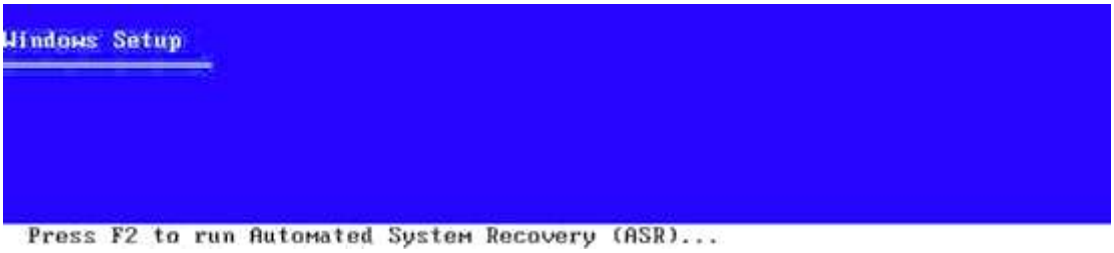
نصب با یک صفحه آبی شروع می شود و با انتخاب پارتیشن مربوطه و نحوه فایل سیستم و غیره ادامه پیدا می کند؛ که ما از ابتدا با شماره گذاری مراحل ادامه می دهیم.

۱. روشن کردن کامپیوتر در حالی که Boot شدن سیستم از طریق CD-Rom می باشد.

۲. در این مرحله اگر خواهان نصب ابزارهای SCSI هستید، باید کلیدF6 را فشار دهید و فلاپی را داخل فلاپی درایو قرار دهید تا درایورهای مورد نیاز آن بر روی فلاپی ریخته شود.



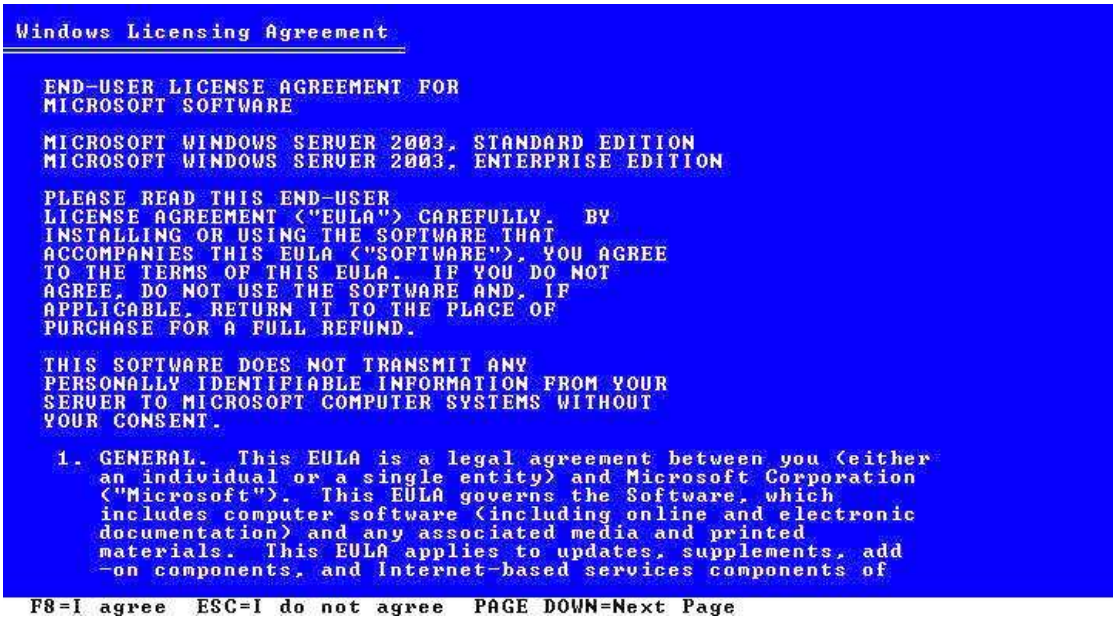
۳. اگر بخواهید رشته ASR را اجرا کنید کافیست در این مرحله کلید F2 را فشار دهید.



۴. در این مرحله نصب تمام فایلها و درایورها، بار گذاری می شود.

۵. حال به شما اجازه داده می شود که اگر از قبل بر روی کامپیوتر خود سیستم عامل دیگری داشته اید، آن را با فشار دادن کلید R تعمیر کنید و اگر می خواهید تازه سیستم عامل نصب کنید. کافیست با فشار دادن کلید ENTER، ادامه دهید.

۶. مرحله بعدی خواندن شرایط نرم افزار و فشار دادن کلید F8 برای قبول شرایط است.



۷. حال نوبت انتخاب پارتیشن مورد نظر برای نصب ویندوز است که نحوه انتخاب آن به شرایط زیر بستگی دارد.

الف) اگر هارد شما به کلی پارتیشن بندی نشده باشد، شما در این حالت می توانید پارتیشن مورد نظر را درست کرده و سپس ویندوز را بر روی آن نصب کنید.

ابتدا پارتیشنی که UnPartitioned است را انتخاب نمایید.

سپس اندازه جدید پارتیشن را وارد نمایید.

پارتیشن جدید را اندازه وارد شده، ساخته می شود.

ب) اگر هارد شما از قبل پارتیشن بندی شده باشد و آن پارتیشن بندی مورد قبول شما باشد می توانید ویندوز را بر روی پارتیشن مورد نظر نصب کنید.

ج) اگر پارتیشن بندی مورد تمایل نباشد، می توانید پارتیشن ها را پاک کرده و دوباره پارتیشن بندی کنید و سپس ویندوز را بر روی آن پارتیشن نصب کنید. (حذف پارتیشن با دکمه D انجام می گیرد)

۸. در این مرحله باید نوع فایل سیستم خود را در هنگام فرمت کردن انتخاب کنیم. ویندوز ۲۰۰۳ با فایل سیستمهای NTFS- FAT32- FAT کار می کند. ولی باید بدانیم اگر می خواهیم سیستم عامل دیگری به غیر از ۲۰۰۳ از هارد ما استفاده کند، مثل ویندوز ۹۸ که NTFS را پشتیبانی نمی کند باید نوع فایل سیستم خود را FAT یا FAT32 انتخاب کنیم و گرنه NTFS بهترین گزینه می باشد.

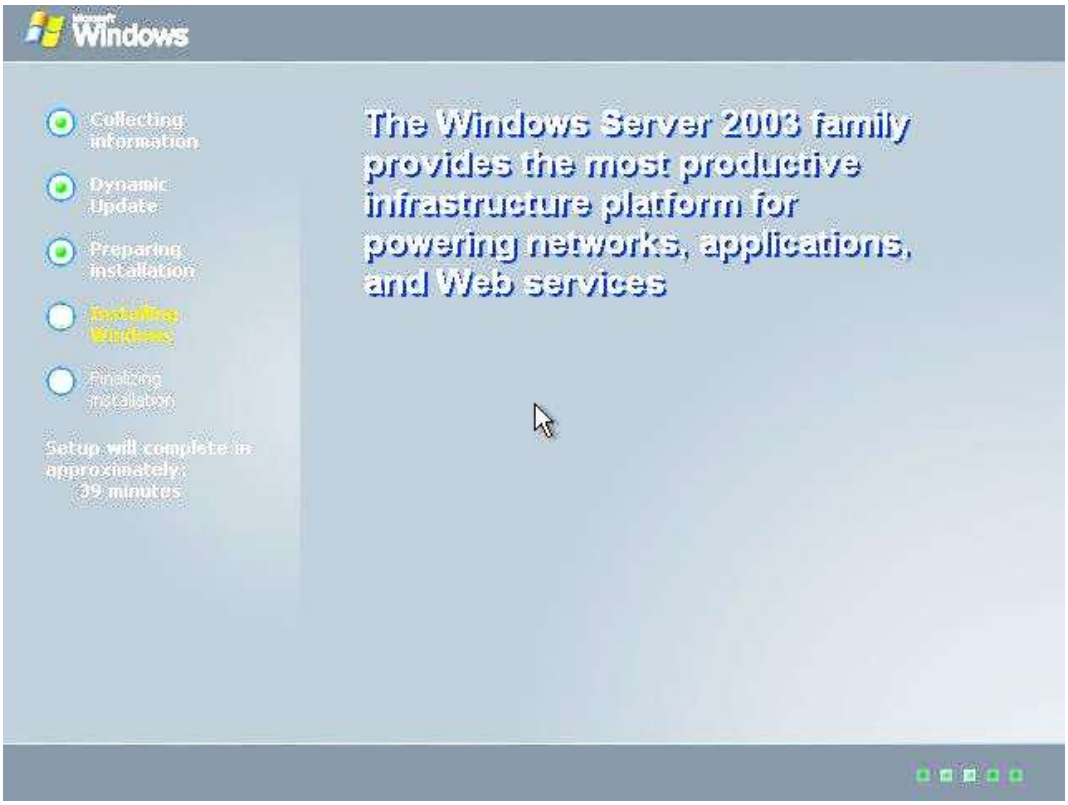
در این مرحله شما حق انتخاب فرمت به صورت سریع و کند را دارید که بر اساس میلتان می توانید یک حالت را انتخاب کنید.

۹. بعد از گذشت مرحله قبل حالا نوبت مرحله ای است که فایلهای مرد نظر باید از منبع نصب کپی شود.

۱۰. بعد از کپی فایل های مورد نیاز که به صورت اتوماتیک انجام می گیرد سپس کامپیوتر RESTART شده و در مرحله گرافیکی نصب ادامه پیدا می کند.

۱۵-۳- مرحله نصب گرافیکی GUI

بعد از Restart شدن کامپیوتر، نصب ادامه پیدا می کند. در ابتدا نصب کننده مشغول بار گذاری درایور ها می شود. بسته به اینکه چه سخت افزاری را در کامپیوتر پیدا کند که در این مرحله ما نیاز نیست که کاری انجام دهیم.

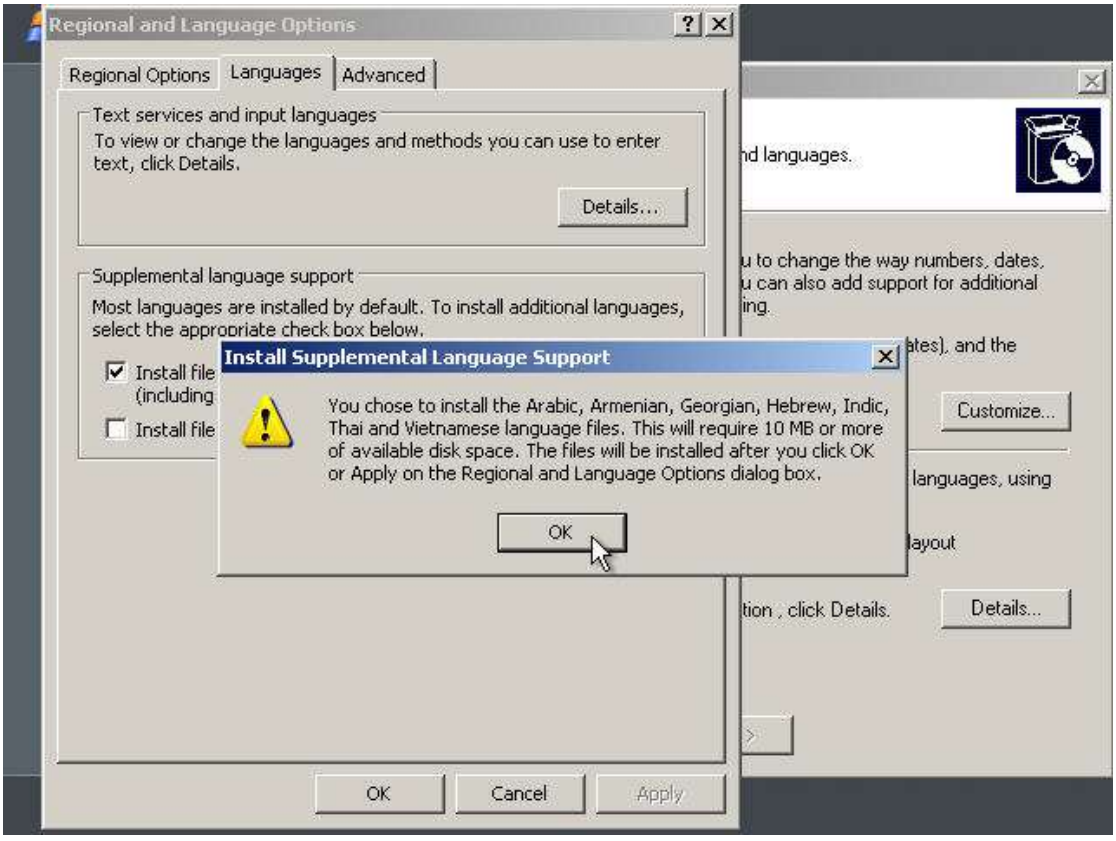


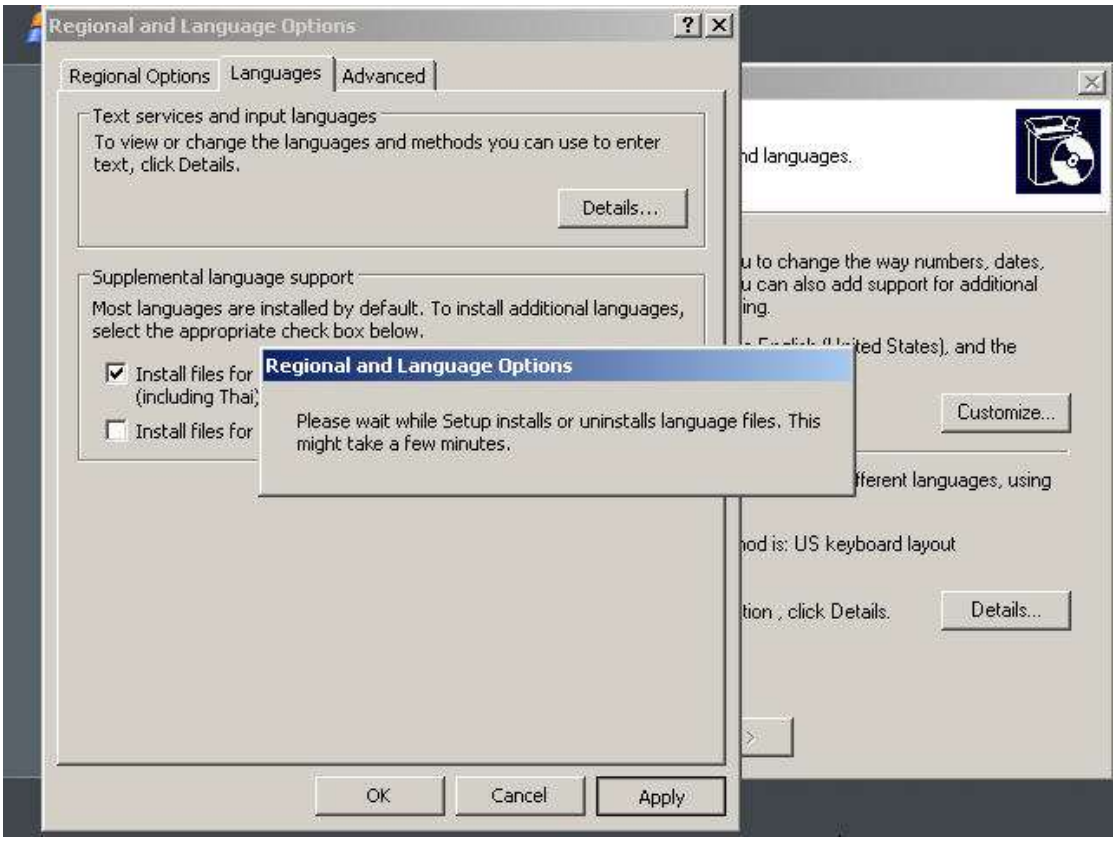
صبر نمایید تا عملیات نصب پیش برود.

۱. سپس صفحه زیر ظاهر می شود و دکمه CUSTOMIZE را فشار می دهیم که در این مرحله می توانیم بر اساس موقعیت جغرافیایی خود تاریخ- زمان –زبان - اعداد و نوع صفحه کلید و چیزهای مربوط به منطقه جغرافیایی را تنظیم می کنیم

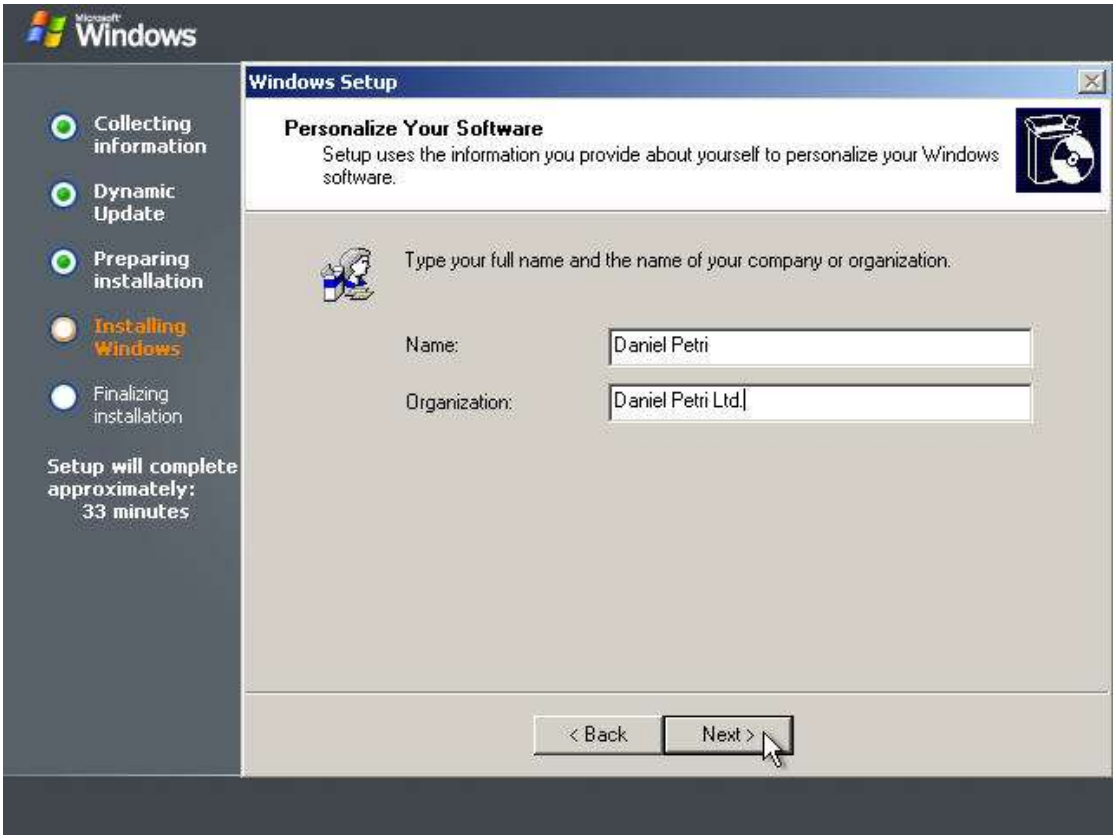
نکته:

برای ما که در منطقه آسیا زندگی می کنیم باید تیک مربوط به انتخاب زبان مربوط به آسیا را انتخاب می کنیم که سپس یک پیغام ظاهر می شود که با OK کردن ادامه می دهیم سپس Apply کردن NEXT را می زنیم.

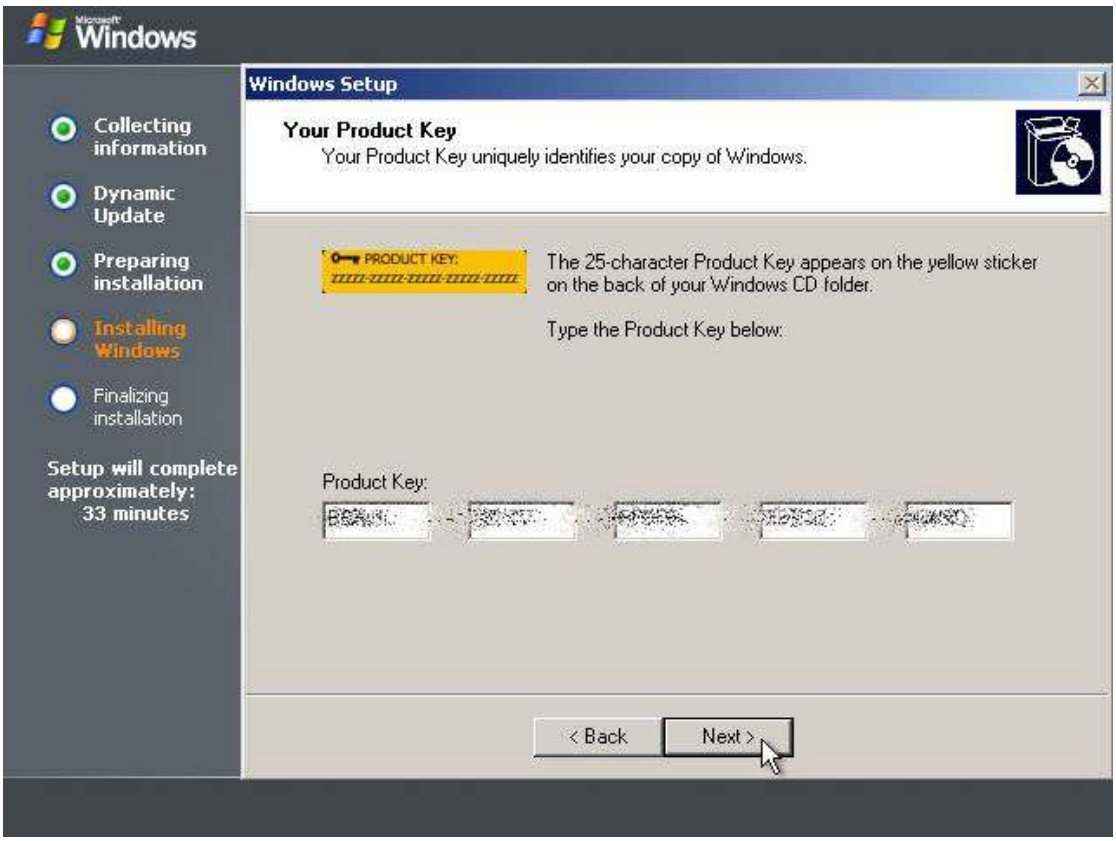




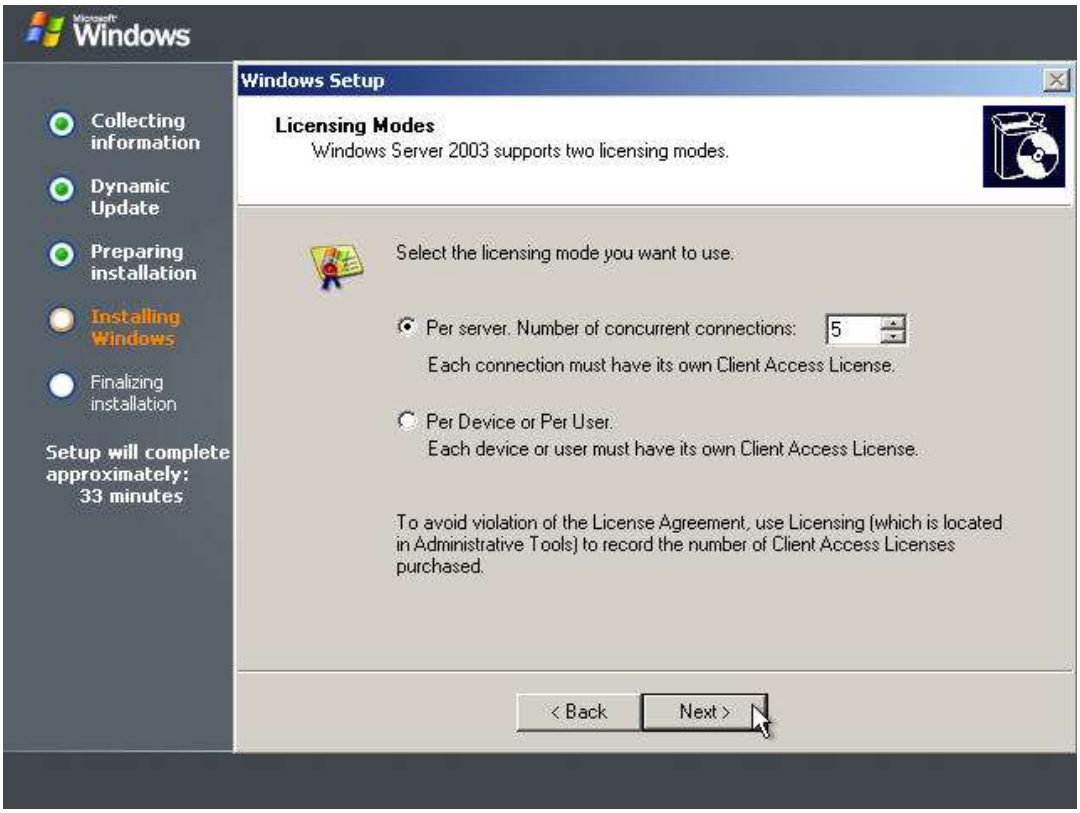
۲. در این مرحله نام و ارگان مربوطه را وارد می کنیم.



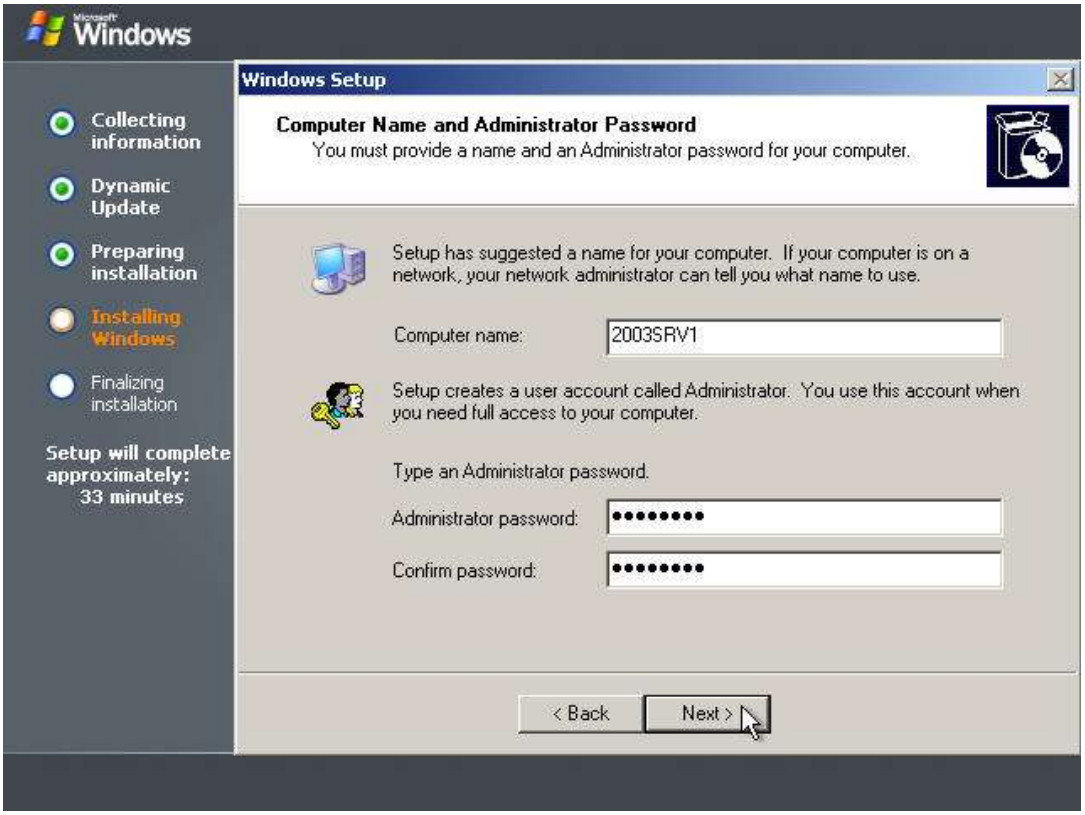
۳. سپس شماره سریال ویندوز را وارد می کنیم



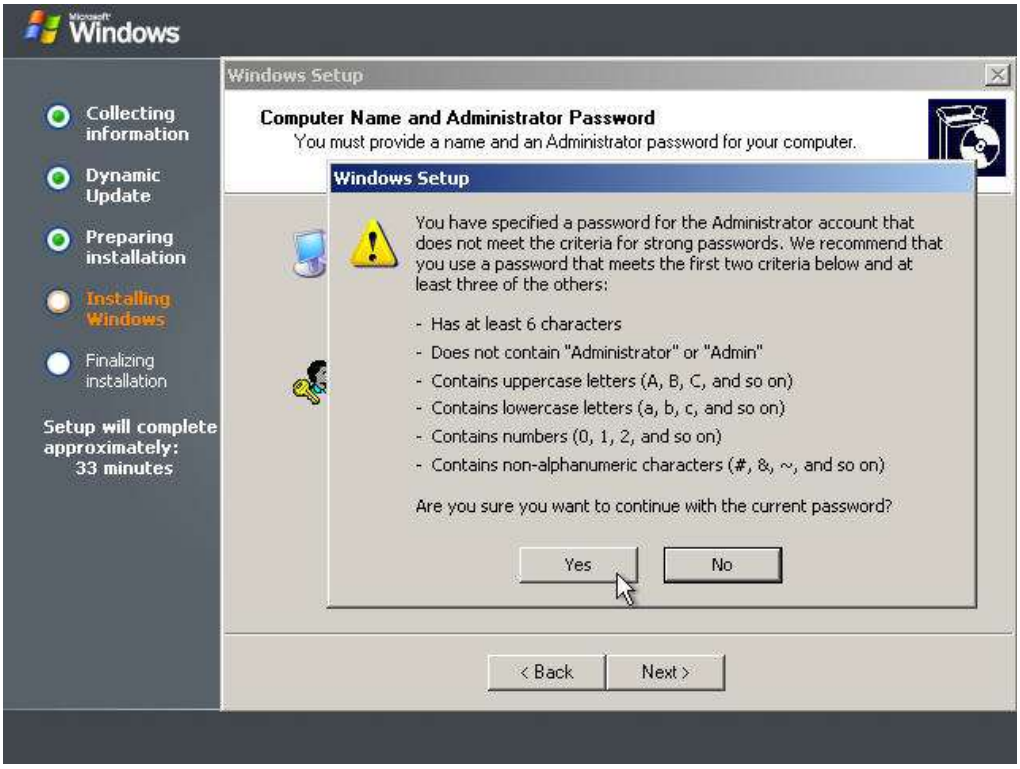
۴. در این مرحله از ما تعداد و نوع مجوز محصول را از ما می پرسد. یعنی اینکه فقط مجوز ویندوز ۲۰۰۳ را می خواهیم و برای هر کلاینت مجددا مجوز خریداری می کنیم و یا اینکه مجوز یک ۲۰۰۳ و مثلاً ۵۰۰ کلاینت را داریم.



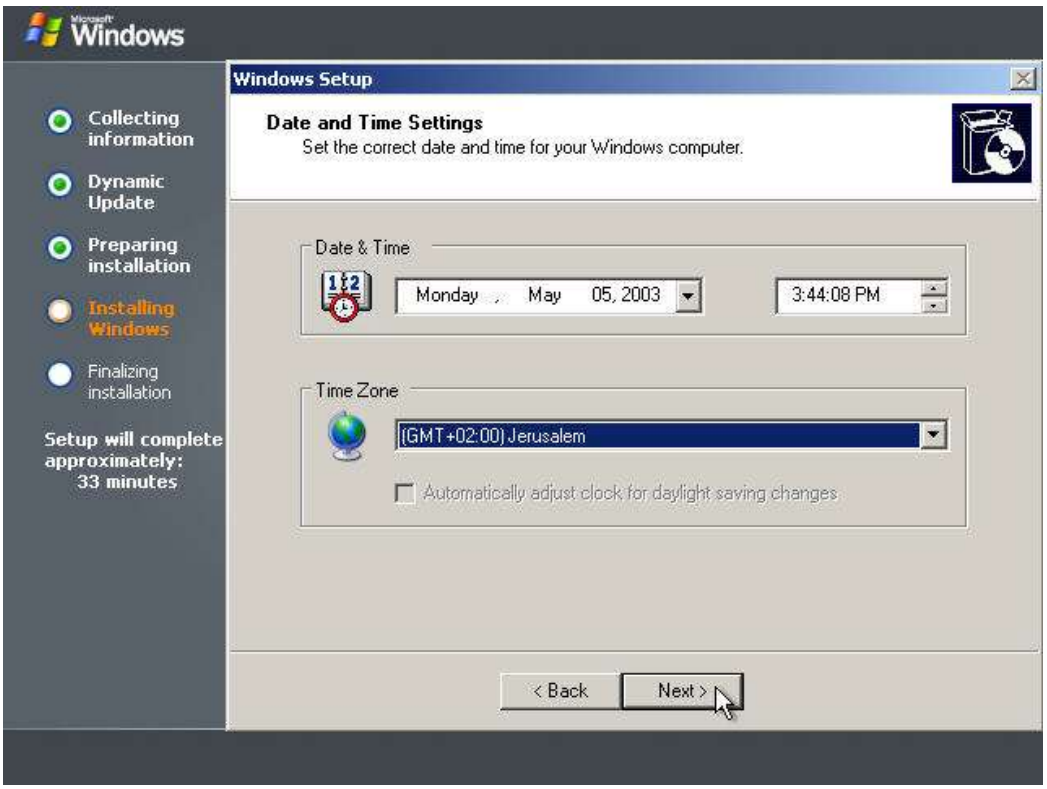
۵. مرحله پنجم مرحله تعیین نام کامپیوتر و انتخاب رمز داخلی Administrator است.



۶. اگر رمز را وارد نکنیم و یا اشتباه وارد کنیم (در CONFIRM) یک پیغام خطا دریافت خواهید کرد تـا درسـتش را وارد کنید.

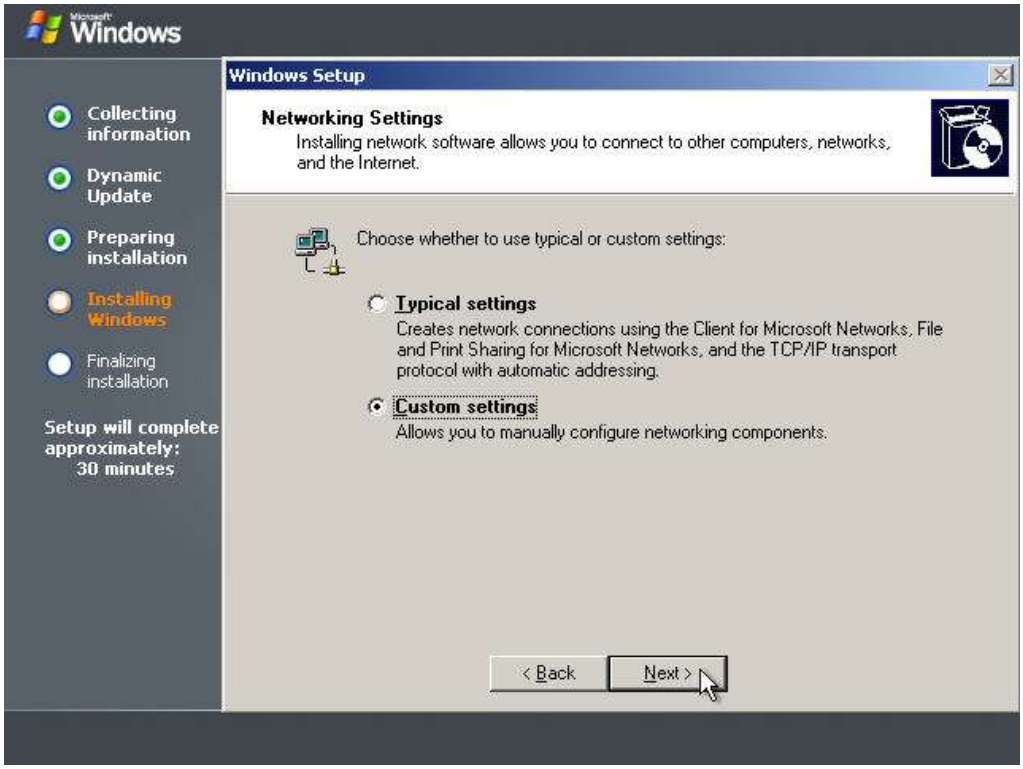


۷. روز - زمان و TIME ZONE را تعیین می کنیم.

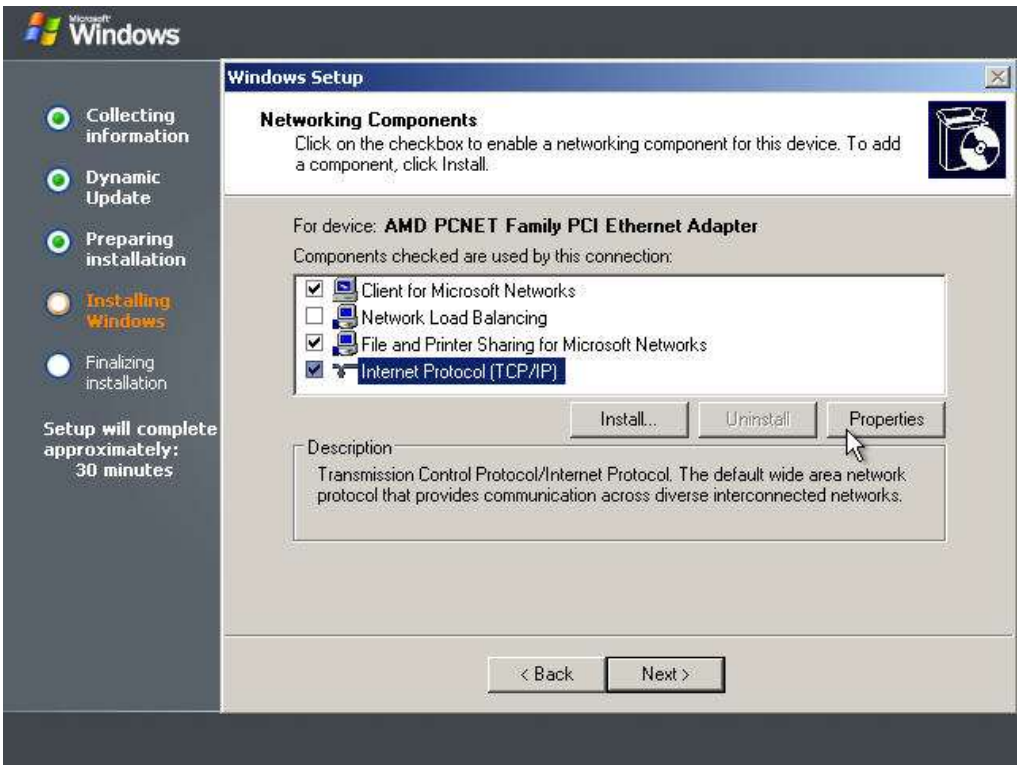


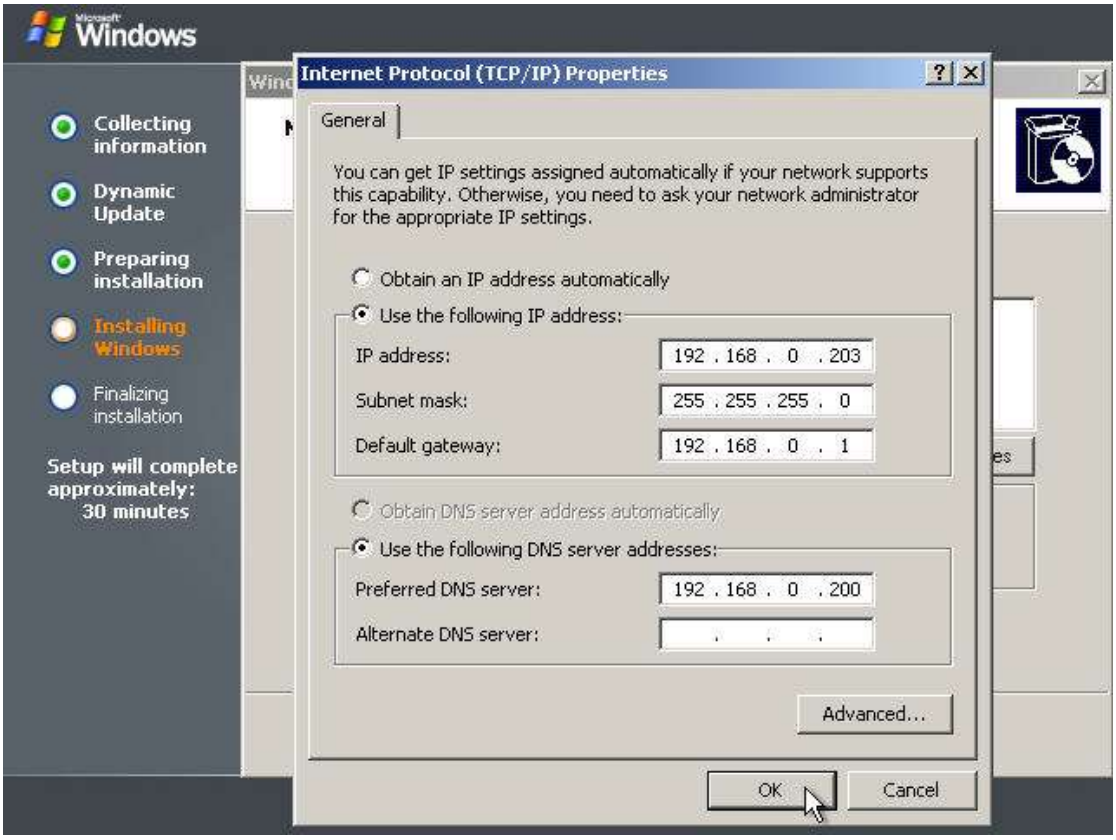
۸. نصب در این مرحله اجزا شبکه را نصب می کند.

اگر کارت شبکه داشته باشیم و ویندوز بتواند آن را تشخیص دهد یک صفحه مربوط به تنظیمات شبکه باز می شود. اگر تنظیم خاصی مد نظر شما نیست با انتخاب TYPCAL مراحل نصب را ادامه می دهیم و گرنه CUSTOM را انتخاب می کنیم.

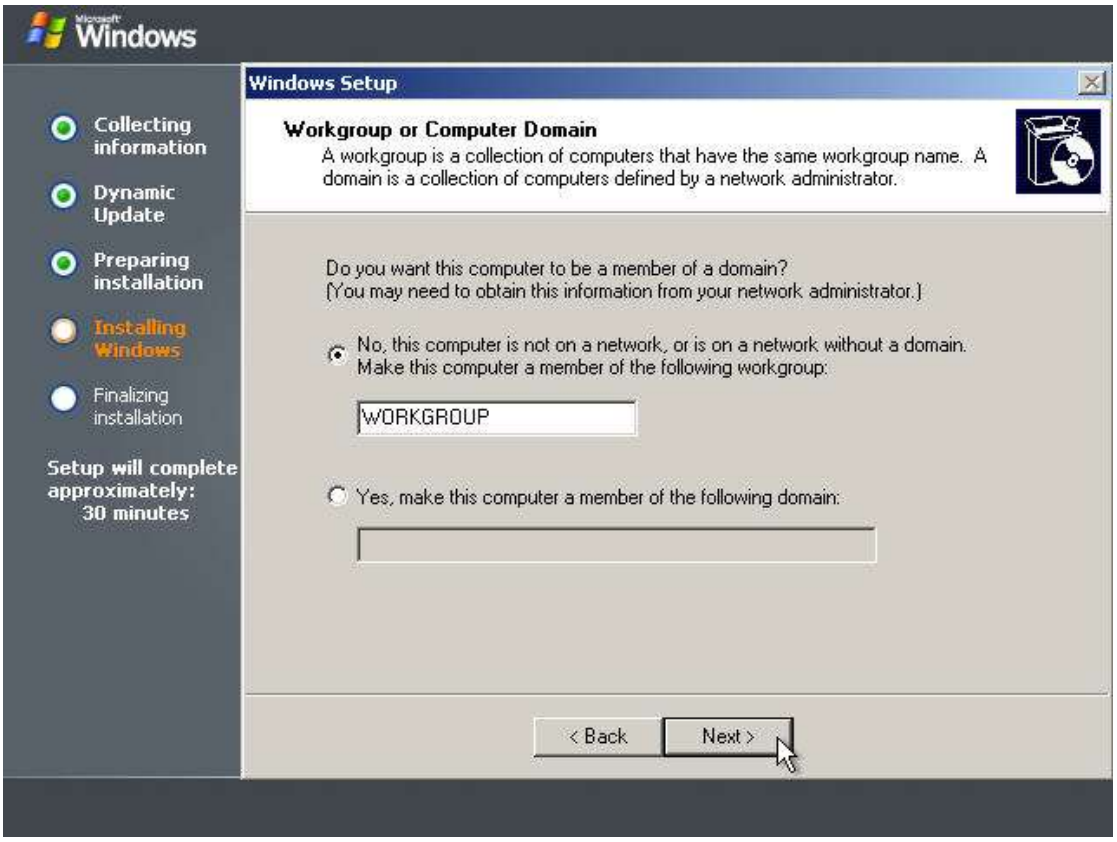


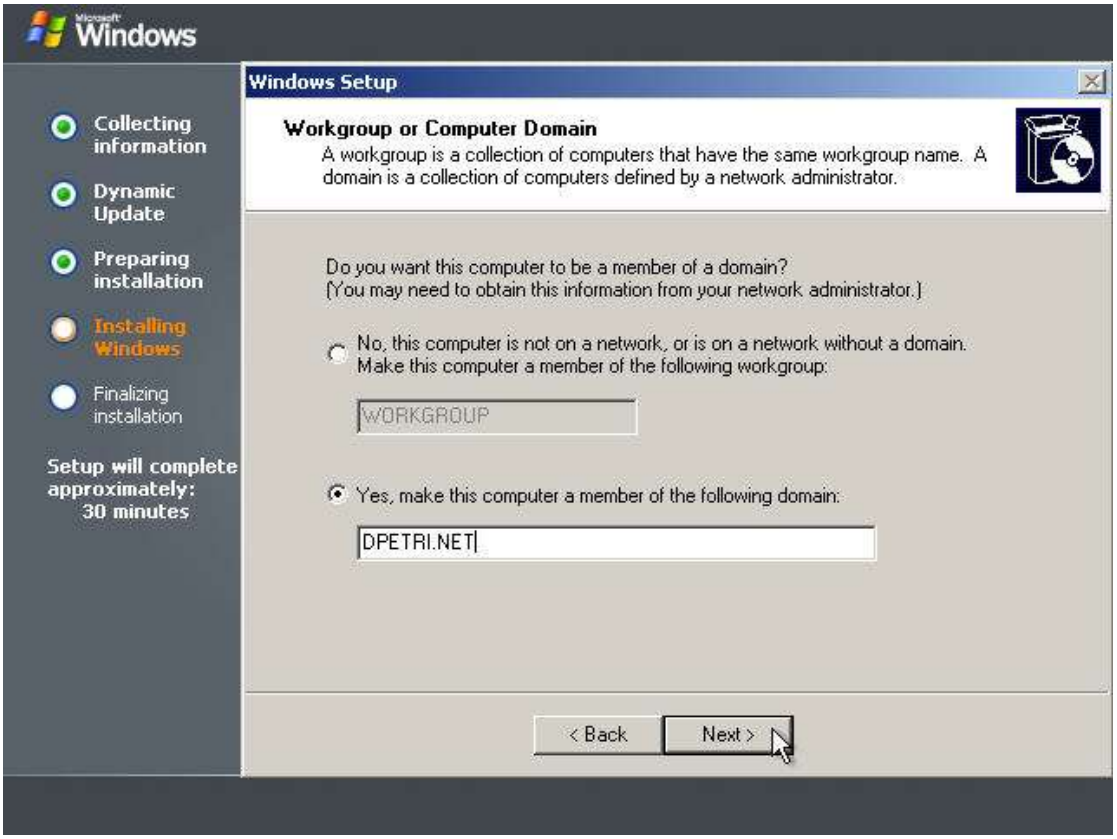
اگر Custom را انتخاب کنید صفحه ای باز می شود که می توانید تنظیماتی را انجام دهید از جمله با بردن Highlight بر روی TCP/IP و زدن کلید Properties می توانید IP کامپیوتر خود و Subnet Mask مربوطه را تعیین کنید و به آن مقدار بدهید.

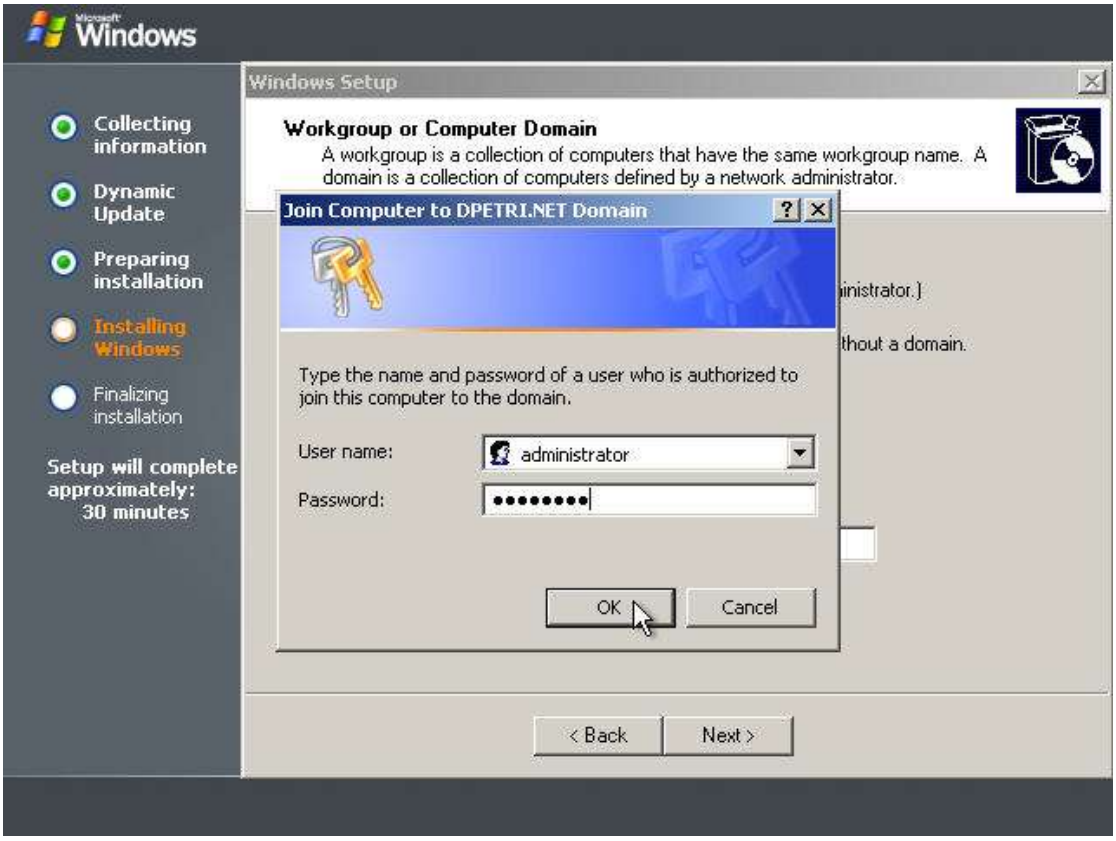




۹. در اینجا اگر می خواهید کامپیوتر را عضو یک Work Group و یا Domain کنید، باید اسم work group یـا Domain مربوطه را وارد کرده و سپس مراحل مربوط به اتصال ویندوزXP به Domain گفته شد را ادامه مـی دهـیم و گـر نـه تنظیمات پیش فرض را انتخاب کرده و ادامه می دهیم.

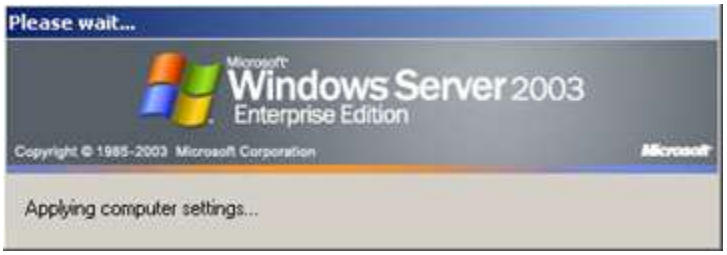

Windows
Windows Setup
Collecting information
Dynamic Update
Preparing installation
Installing Windows
Finalizing installation
Setup will complete approximately: 30 minutes
Workgroup or Computer Domain
A workgroup is a collection of computers that have the same workgroup name. A domain is a collection of computers defined by a network administrator.
Do you want this computer to be a member of a domain?
(You may need to obtain this information from your network administrator.)
No, this computer is not on a network, or is on a network without a domain.
Make this computer a member of the following workgroup:
WORKGROUP
Yes, make this computer a member of the following domain:
< Back
Next >

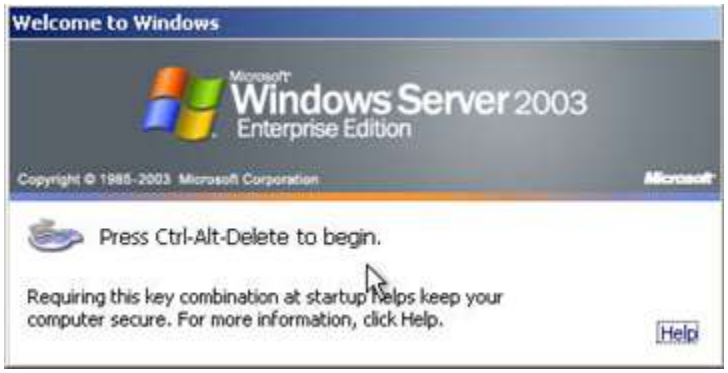

Windows
Windows Setup
Collecting information
Dynamic Update
Preparing installation
Installing Windows
Finalizing installation
Setup will complete approximately: 30 minutes
Workgroup or Computer Domain
A workgroup is a collection of computers that have the same workgroup name. A domain is a collection of computers defined by a network administrator.
Do you want this computer to be a member of a domain?
(You may need to obtain this information from your network administrator.)
No, this computer is not on a network, or is on a network without a domain.
Make this computer a member of the following workgroup:
WORKGROUP
Yes, make this computer a member of the following domain:
DPETRI.NET
< Back
Next >



۱۰. دیگر تا کپی کردن فایلها و تنظیمات مربوطه مراحل نصب نیازی به انجام کاری نیست تا مراحل نصب به صورت اتوماتیک تمام شود و کامپیوتر دوباره راه اندازی شود و این تمام کارهایی بود که ما برای نصب ویندوز ۲۰۰۳ نیاز بود انجام دهیم.

و در نهایت کامپیوتر با سیستم عامل ویندوز ۲۰۰۳ بالا آمده و پس از پرسیدن رمز Administrator وارد ویندوز می شود.





پس از باز شدن صفحه فوق، کلید های Ctrl+Alt+Delete را فشار دهید تا صفحه دریافت نام کاربری و رمز عبور نمایان شود. نام کاربری و رمز عبور را وارد کرده و با فشردن دکمه OK وارد ویندوز شوید.

فصل ۱۶

User , Group , Organizational Unit

User –۱–۱۶

احتمالا تا کنون با مفهوم کاربر (User) آشنا شده اید. هر کاربر بیانگر یک فرد است که قابلیت کارکردن با سیستم را دارد. به عبارت دیگر، شما می توانید به هر فردی یک حساب کاربری (Username و احتمالا Password) تخصیص داده و تعیین کنید که این فرد با این حساب کاربری از کدام سیستم ها می تواند استفاده کند. البته کاربرد های User بالاتر از این است. مدیران سیستم می توانند سطح دسترسی خاصی برای کاربر تعیین کرده و بدین ترتیب محدودیت ها یا خط مشی ها را بر روی کاربر اعمال نمایند. به عنوان مثال یک نرم افزار فروش را در نظر بگیرید که چند کاربر با آن کار می کنند، مانند صاحب فروشگاه، مدیر مالی و فروشنده. حال این صحیح نیست که سطوح دسترسی آن ها با هم برابر باشد. به عنوان مثال مدیر سیستم حق دارد تعیین کند که چه کسانی از سیستم استفاده کنند (تعیین کاربران)؛ مدیر امور مالی می تواند حقوق کارمندان را تعیین کند و این درست نیست که فروشنده قابلیت تغییر حقوق را داشته باشد. همین بحث در مورد User و در سیستم عامل ها نیز وجود دارد. User یعنی یک نام کاربری (و احتمالا رمز عبور) و سطوح دسترسی کاربر که توسط مدیران سیستم تعیین می گردد. به عبارت دیگر، هر نام کاربری، بیانگر شخصی است که قابلیت انجام کارهایی خاص و از پیش تعیین شده را دارد. در سیستم عامل ویندوز، کاربران زیادی وجود دارد که در یک دید کلی می توان آن ها را به دو دسته تقسیم کرد:

۱. کاربران پیش فرض (مانند Administrator و Guest)
۲. کاربرانی که بعدا ایجاد می شوند.

به هنگام نصب ویندوز، دو کاربر Administrator و Guest به صورت اتوماتیک بر روی ویندوز ایجاد می شوند. این ۲ کاربر را نمی توانیم پاک کنیم. اما بر حسب نیاز مدیر می شود آنها را تغییر نام داد. کاربر Guest به صورت پیش فرض غیر فعال هست و دارای پایین ترین سطح دسترسی می باشد.

نکاتی که به هنگام ایجاد یک User Account باید رعایت کنیم:

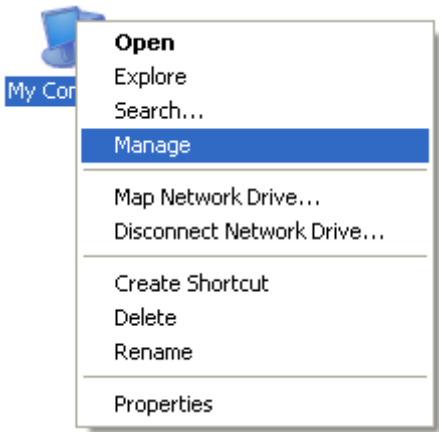
۱. اسامی آن منحصر به فرد باشد.
۲. به هنگام ایجاد User، اسم User تا بیش از ۲۰ کاراکتر نمی تواند باشد.

۳. برای ایجاد حساب از بعضی کاراکتر ها نمیتوان استفاده کرد. / { } $#@ + = و....

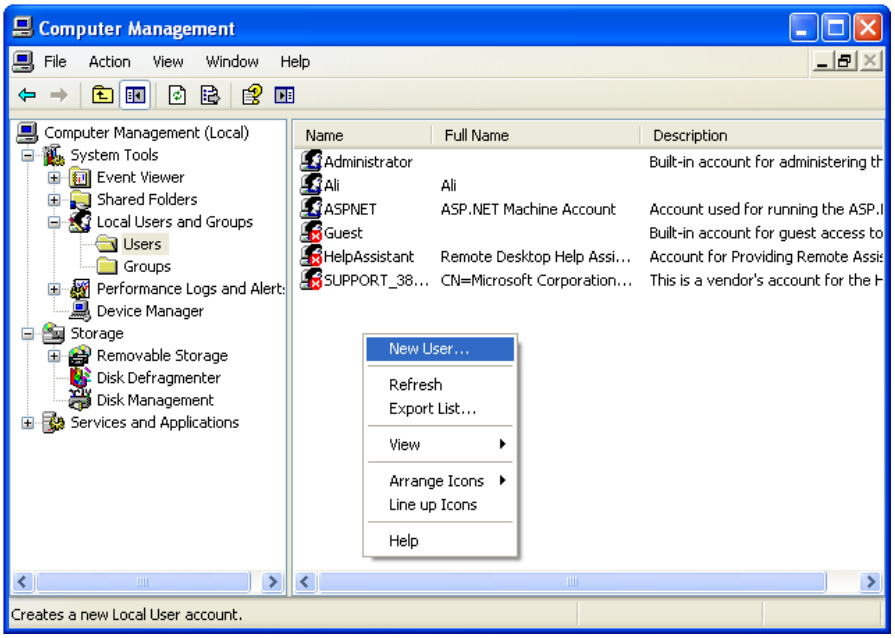
۴. اسامی کاربر با حروف بزرگ یا کوچک فرقی ندارد، اما Password فرق دارد.

۱۶-۲- نحوه ساخت کاربر

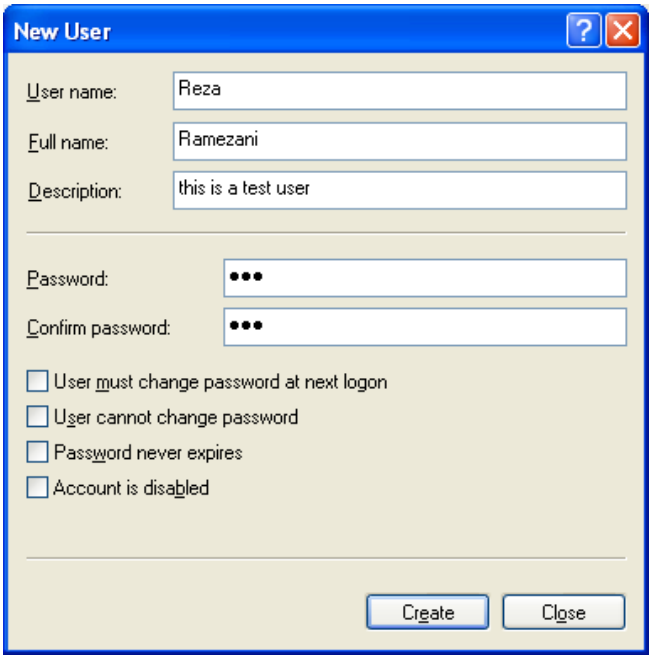
اگر از ویندوز XP استفاده می کنید، یا اگر در ویندوز سرور هستید، اما هنوز Active Directory را نصب نکرده اید، وارد مسیر زیر شود: ابتدا روی My Computer راست کلیک کرده و سپس گزینه Manage را انتخاب کنید.



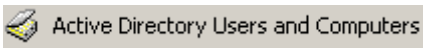
سپس در صفحه باز شده، ابتدا وارد Local Users and Groups شده و سپس وارد قسمت Users شوید. در اینجا منظور از کلمه Local این است که کاربران تعریف شده در این قسمت فقط در حالت محلی معتبر اند؛ یعنی افراد فقط زمانی می توانند از این نام کاربری استفاده کنند که بخواهند به صورت محلی از همین سیستم استفاده کنند. برای ساخت کاربر در جای خالی صفحه راست کلیک کرده و گزینه New User را انتخاب کنید.



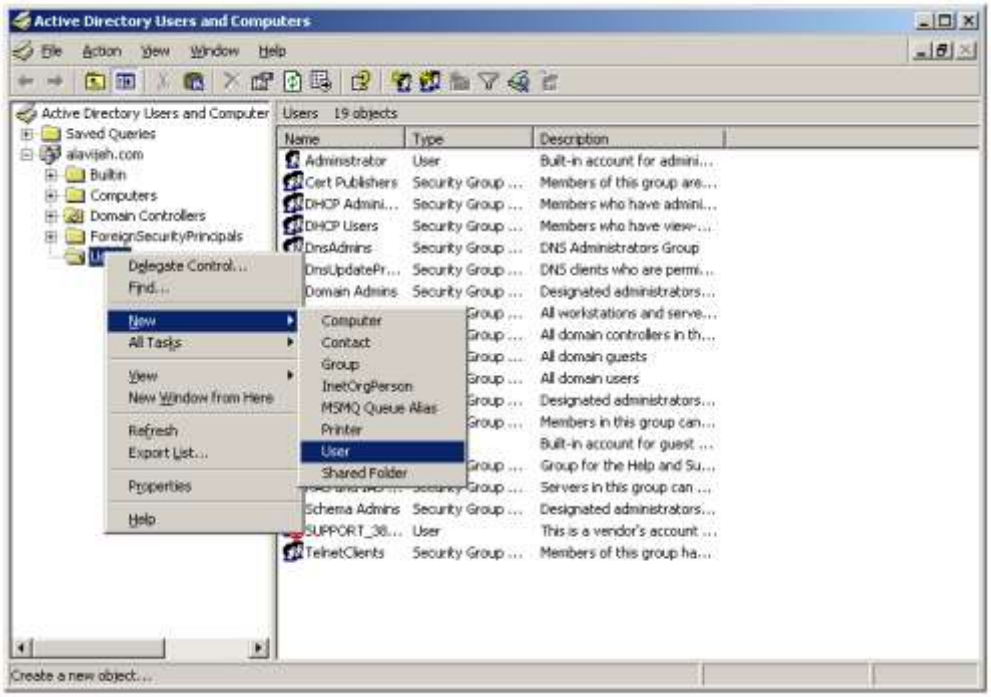
سپس در صفحه باز شده، اطلاعات کاربر، نظیر نام کاربری و رمز عبور را وارد کرده و سپس روی Create کلیک کنید.



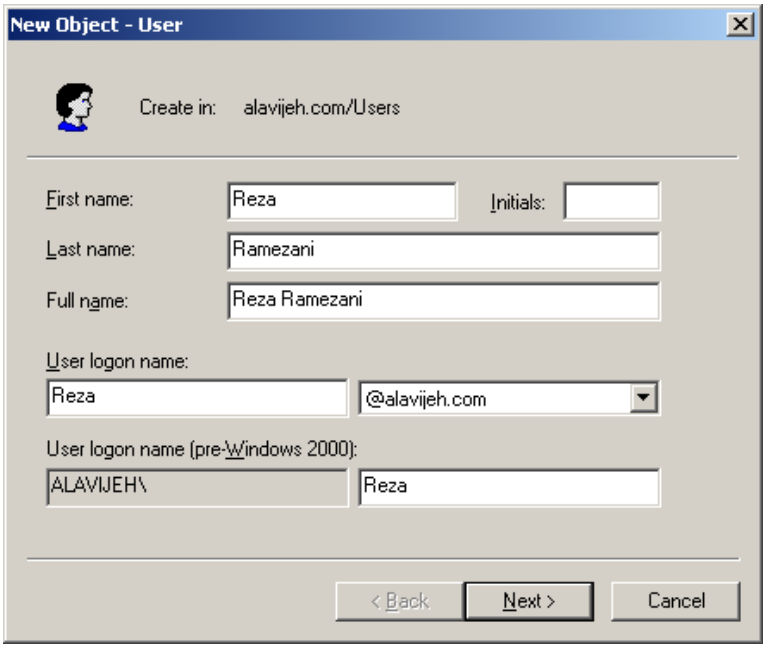
اما اگر از ویندوز سروری استفاده می کنید که Active Directory روی آن نصب است (در مورد Active Directory در فصل های بعد صحبت خواهیم کرد)، روش و محل تعریف Userها کمی متفاوت است. در این حالت، کاربران تعریف شده، هم در حالت محلی و هم در شبکه Domain قابل شناسایی است. برای تعریف کاربر، از منوی Start، گزینه Administrative Tools و سپس گزینه Active Directory Users and Computers را انتخاب نمایید.



سپس در صفحه باز شده، قسمتی که نام دامنه را نشان می دهد، بسط داده، روی قسمت Users راست کلیک کرده و سپس New ➔ User را انتخاب نمایید.



سپس در قسمت بالا، نام و نام خانوادگی کاربر را وارد نمایید. سپس در قسمت User logon name، نام کاربری کاربر که هنگام ورود به سیستم باید وارد کند را در این قسمت وارد نمایید. سپس روی Next کلیک کنید.



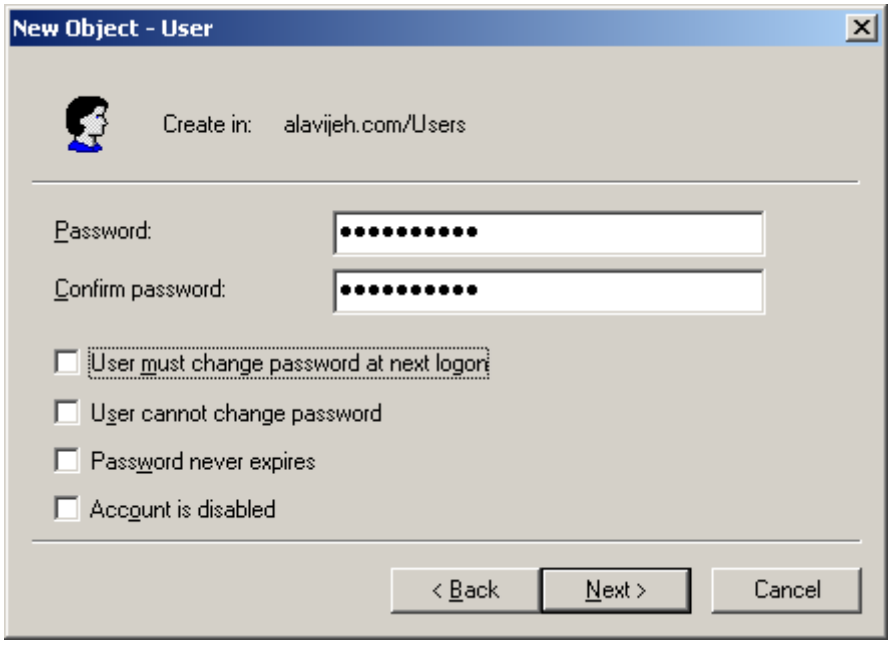
سپس در این صفحه، رمز عبور کاربر را وارد نمایید. توجه نمایید که در ابتدا به صورت پیش فرض، در ویندوز سرور، رمز عبور بایستی دارای حداقل ۷ حرف بوده و نیز به صورت Complex (پیچیده) باشد (این تنظیمات در Group Policy تعیین می گردد که بعدا در مورد آن صحبت خواهیم کرد). در این مثال ما رمز عبور را abc@abc123 وارد کردیم. در زیر ۴ گزینه وجود دارد که به توضیح مختصر آن می پردازیم:

۱. **User must change password at next logon:** با فعال کردن این گزینه، سیستم کاربر را مجبور می کند که هنگام **اولین** Login به سیستم، رمز عبور خود را تغییر دهید. **توجه:** اگر بخواهید سیستمی را به Domain خود Join کنید و هنگام Join کردن از این نام کاربری استفاده کنید؛ و همچنین اگر تاکنون با این کاربر Login نکرده اید و این گزینه را نیز فعال کرده باشید، سیستم اجازه ورود شما را خواهد گرفت.

۲. **User cannot change password:** با فعال کردن این گزینه، کاربر قادر به تغییر دادن رمز عبور خود نخواهد بود. بهتر است این گزینه را غیر فعال کنید.

۳. **Password never expires:** با فعال کردن این گزینه، رمز عبور کاربر هیچ گاه منقضی (Expire) نخواهد شد. در غیر اینصورت به صورت پیش فرض، پس از ۴۲ روز، کاربر مجبور به تغییر رمز عبور خود است. علت این امر بالا بردن امنیت رمز عبور است.

۴. **Account is disabled:** با فعال کردن این گزینه، کاربر غیرفعال شده و قابلیت ورود به سیستم را از دست خواهد داد.



در مرحله آخر، اطلاعات مختصری در مورد کاربر را مشاهده خواهید نمود. برای ساخت کاربر، روی دکمه Finish کلیک نمایید.

بدین ترتیب کاربر مورد نظر ساخته شده و قابلیت استفاده از آن را با رمز عبور تعیین شده دارید.

Group -۳-۱۶

مفهوم گروه در یک عبارت ساده می شود "مجموعه ای از کاربران". اما بهتر است بدانید که گروه چه کاربردی دارد؟ فرض کنید که یک نرم افزار فروش، بیش از ۱۰۰۰ قابلیت مختلف دارد که می توان به هر کاربری، قابلیت کارکردن با برخی از این امکانات را داد. حال فرض کنید که ما ۱۰۰ فروشنده داریم و این فروشنده ها بایستی با ۴۵۰ تا از امکانات این نرم افزار کار کنند (که مدیر آن را تعیین می کند). بدین منظور ما بایستی ۴۵۰۰۰ = ۱۰۰ * ۴۵۰ خصوصیت برای سطح دسترسی تعیین کنیم. حال بهترین ایده این است که ما **یک گروه** تعریف کنیم و این سطوح دسترسی را برای این گروه تعیین نماییم. سپس می توان کاربران مورد نظر را تعریف کرده و این کاربران را عضو این گروه کرد. بدین ترتیب، این گروه هر سطح دسترسی که داشته باشد، این سطح دسترسی به کاربران موجود در گروه نیز اعمال خواهد شد. و با انجام این کار، ما فقط ۴۵۰ خصوصیت برای سطح دسترسی تعیین می کنیم. البته می توان مثلاً ۱۰ گروه تعریف نمود و سطح های دسترسی متفاوت برای هر گروه مشخص کرد؛ سپس کاربران را عضو این گروه ها نمود. بدین ترتیب کاربر جزء هر گروهی که باشد، سطح دسترسی آن را به ارث می برد.

گروه ها قابلیت های مختلفی دارند، مانند:

۱. می توانند عضو گیری کنند.
۲. می توانند اعضای خود را حذف کنند.

۳. هر گروه می تواند عضو گروه دیگری شود.
۴. به برخی از اعضای خود سطح دسترسی خاصی (متفاوت با دیگر اعضای گروه) بدهند.

فقط توجه فرمایید که زمانی که گروهی عضو گروهی دیگر شود، گروه فرزند نمی تواند سطح دسترسی بیشتر از سطح دسترسی گروه پدر داشته باشد. فرض کنید که گروه G1 قابلیت استفاده از GB۵ فضا داشته باشد و گروه G2 نیز عضوی از گروه G1 داشته باشد. حال برای اعضای گروه G2 نمی توان فضایی بیشتر از GB۵ در نظر گرفت. همچنین ذکر این نکته نیز مفید است که در یک لحظه، یک کاربر می تواند عضو چند گروه باشد.

گروه ها نیز مانند کاربران دو دسته اند.

۱. گروه های پیش فرض (مانند Backup Group و Admins Group)
۲. گروه هایی که بعدا (به منظور های مختلفی) ایجاد می شوند.

البته دسته بندی های دیگری نیز برای گروه وجود دارد.

یکی از انواع گروه که می توان در ویندوز Server ایجاد کرد، Local Group است که این Local Group به ۲ دسته تقسیم می شود:

گروه اول توسط مایکروسافت از قبل پیش بینی و طراحی شده که به عنوان Built in local group ایجاد شده و گروه دوم Built-in system group هست. حالا معرفی این ۲ گروه:

Built-In Local Group -۱-۳-۱۶

۱- Administrators:

کاربرانی که عضو این گروه هستند می توانند هر گونه عملیاتی بر روی کامپیوتر انجام دهند. زمانی که یک کامپیوتر را عضو Domain میکنیم، گروه Domain Admin عضو گروه محلی Administrators می شود.

۲- Backup Operators:

اعضای این گروه قادر هستند از تمامی فایل های ویندوز هم Backup بگیرند و هم Restore کنند.

۳- Guests:

گروه مهمان هستند که مجوز و سطح دسترسی محدود تری نسبت به سایرین دارند.

۴- Network Configuration Operators:

اعضای این گروه می توانند کلیه تنظیمات و فرمان های شبکه را اجرا کنند.

۵- Power Users:

اعضای این گروه توانایی ایجاد کاربر جدید و Share کردن منابع را دارند.

۶- Remote Desktop Users:

اعضای این گروه مجوز دسترسی راه دور به کامپیوتر دیگر را در صورت تعریف شدن عملیات Remote دارند.

۷- Replicator Group:

اعضای این گروه در صورت وجود Domain یا در محیط یک شبکه می توانند عملیات Replication و مدیریت فایل ها را انجام دهند.

۸- Users Group:

این گروه می توانند با مجوز تعیین شده به منابع دسترسی پیدا کنند. به صورت Default همه User ها عضو این گروه هستند.

۹- Debugger Users:

اعضای این گروه می توانند هم به صورت Remote هم به صورت Local بر روی کامپیوتر مورد نظر اشکال یابی کنند.

۱۰- Help Service Group:

اعضای این گروه می توانند از کلیه امکانات Help و فرمان های موجود در داخل ان استفاده نمایند. البته این گروه خیلی کشکیه....

۱۶-۳-۲- Built-In System Group

این گروه به صورت Default وجود داشته و نمی توانیم آنها را حذف یا اضافه کنیم. عضویت در این گروه ها را هیچ کس حتی Admin هم نمی تواند مشخص کنه و بسته به حالت های مختلف که هر بار کاربر Login می کند، میتواند عضو یکی از این گروه ها باشد.

انواع گروه Built-In System Group

۱- Every One:

تمامی کاربرانی که به کامپیوتر دسترسی پیدا می کنند، عضو این گروه هستند. ضمن اینکه اگه مجوزی به این گروه بدهیم، شامل همه کاربران اعم از Admin و غیر آن می شود.

۲- Authenticated Users:

کاربرانی که با User name و Password وارد شبکه میشوند جز این گروه هستند.

۳- Anonymous Log On:

کاربرانی که بدون User name و Password وارد شبکه میشوند جز این گروه هستند.

۴- Creator Owner:

زمانیکه هر شیئ ایجاد کنیم، عضو این گروه قرار میگیریم.

۵- Dial up:

هر کاربری که از طریق Dial up وارد شبکه شود عضو این گروه است. (برای اطلاعات بیشتر به فصل "برقراری ارتباط از راه دور" مراجعه فرمایید.)

۶- Interactive Group:

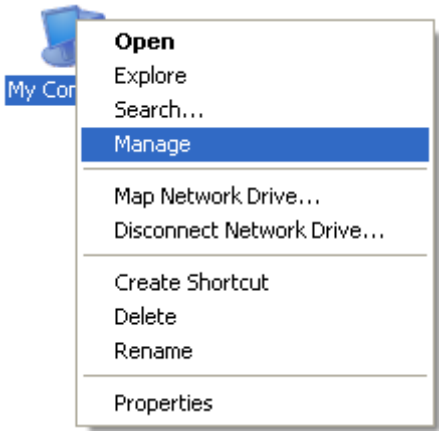
هر User که به صورت Local به کامپیوتر دسترسی پیدا کند عضو این گروه هست.

۷- Network Group:

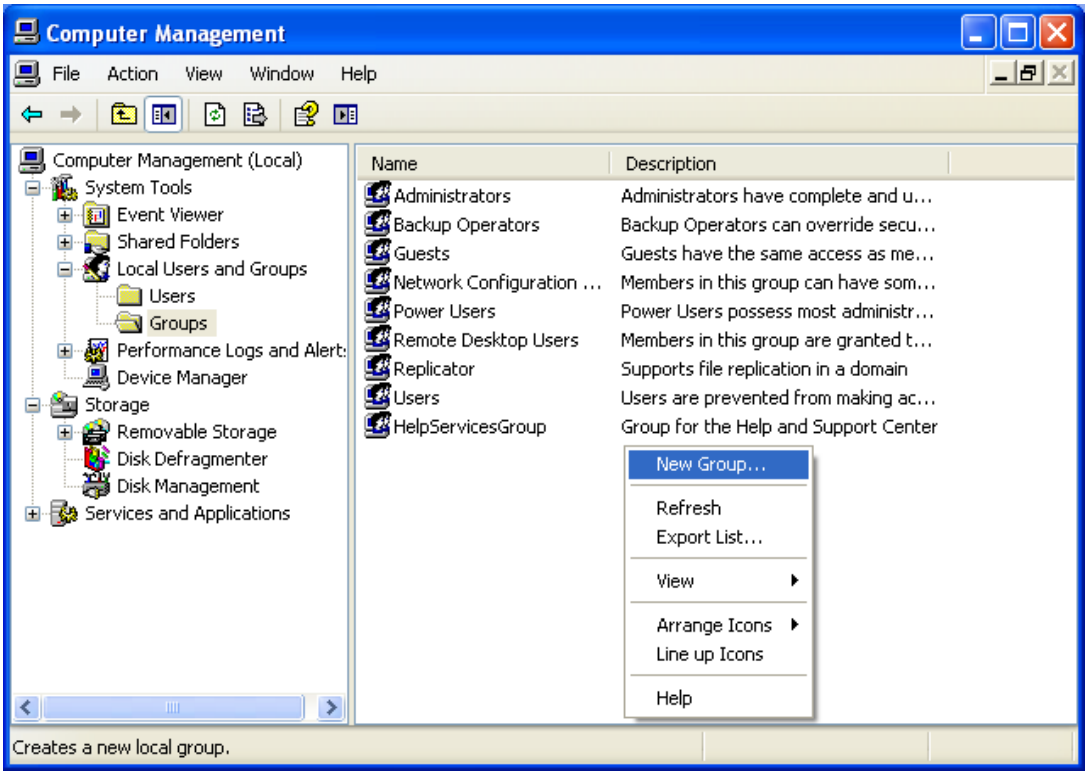
هر User که به صورت شبکه به کامپیوتر یا از طریق کامپیوتر به شبکه وصل شود عضو این گروه قرار میگیرد.

۱۶-۴- نحوه ساخت گروه

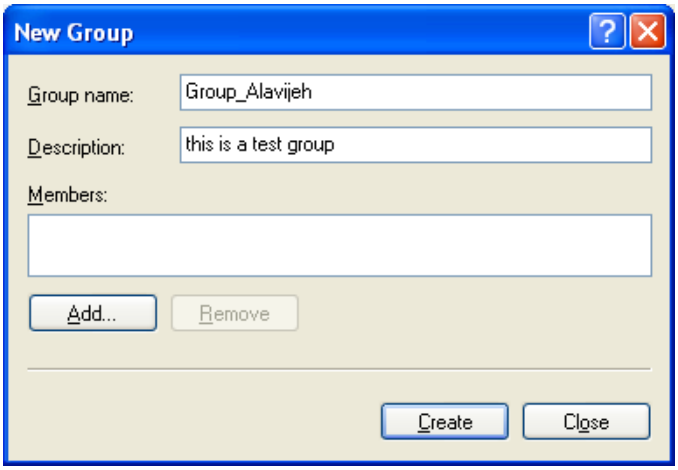
همانند بخش ساخت کاربر، اگر از ویندوز XP استفاده می کنید، یا اگر در ویندوز سرور هستید، اما هنوز Active Directory را نصب نکرده اید، وارد مسیر زیر شود: ابتدا روی My Computer راست کلیک کرده و سپس گزینه Manage را انتخاب کنید.



در صفحه باز شده، وارد Local Users and Groups شده و سپس وارد قسمت Groups شوید. برای ساخت گروه جدید، در جای خالی صفحه راست کلیک کرده و گزینه New Group را انتخاب کنید.

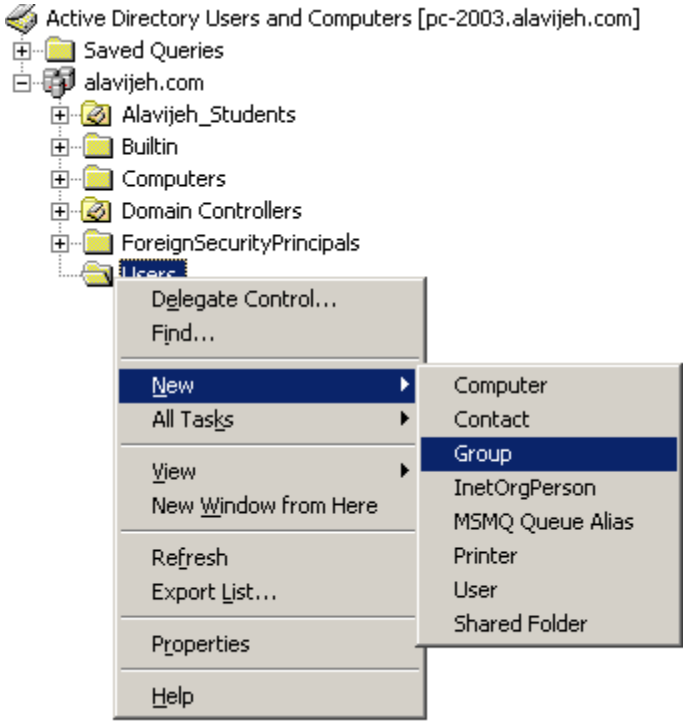


سپس در صفحه باز شده، یک نام و یک توصیف برای گروه خود وارد نمایید. در پایین صفحه این قابلیت وجود دارد که کاربران یا گروه هایی را عضو این گروه کنید. نحوه عضو گیری را جلوتر توضیح می دهیم.

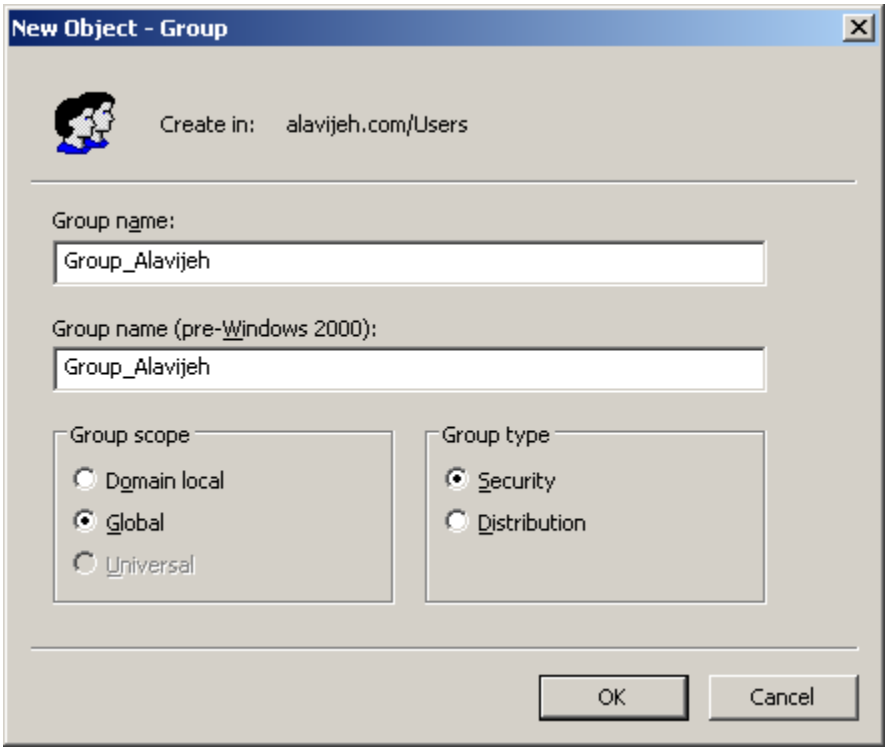


اما اگر از ویندوز سروری استفاده می کنید که Active Directory روی آن نصب است، روش و محل تعریف Group ها کمی متفاوت است. برای تعریف گروه جدید، از منوی Start، گزینه Administrative Tools و سپس گزینه Active Directory Users and Computers را انتخاب نمایید.

سپس در صفحه باز شده، قسمتی که نام دامنه را نشان می دهد، بسط داده، روی قسمت Users راست کلیک کرده و سپس New ➔ Group را انتخاب نمایید.



سپس در صفحه باز شده، نام گروه، توصیف گروه، حوزه کاری گروه و نوع گروه را تعیین نمایید.



حال به توضیح مختصری در مورد حوزه و نوع گروه می پردازیم.

الف) Group Types: بیانگر نوع گروه بوده و گروه ها از این نظر به دو نوع تقسیم می شوند:

۱- Security Groups: گروه های هستند که از آنها بیشتر برای مجوز دادن استفاده می شود. همچنین از این نوع گروه می توان برای ایجاد لیست توزیع E-Mail استفاده نمود.

۲- Distribution Groups: توانایی ایجاد لیست توزیع Email را دارد و از آن نمی توان جهت اعطای مجوزهای دسترسی به منابع استفاده کرد. از اینرو زمانی از این نوع گروه ها استفاده کنید که اعضای آن نیاز به مجوز دسترسی به منابع را نداشته و فقط جهت لیست توزیع E-Mail از آنها استفاده می شود.

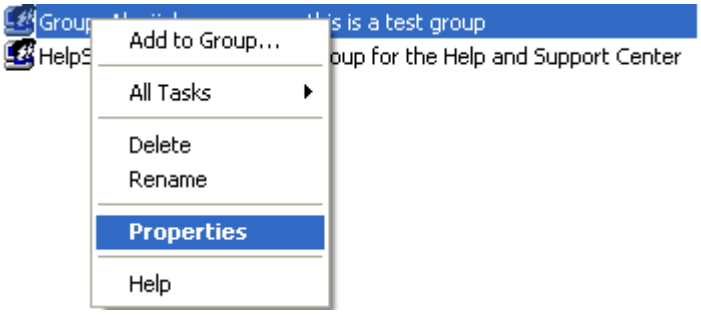
ب) Group Scopes: حوزه و محدوده کاری گروه را مشخص می کند.

۱- Global Groups: گروه هایی هستند که به منظور دسته بندی منطقی کاربران مورد استفاده قرار می گیرند که معمولاً بر اساس نوع کار یا محل جغرافیایی کاربران می باشد. به عنوان مثال می توانید کاربرانی که در واحد فروش کار می کنند را در یک گروه و کاربرانی که در واحد خرید کار می کنند را در گروهی دیگر گروه بندی نمایید.

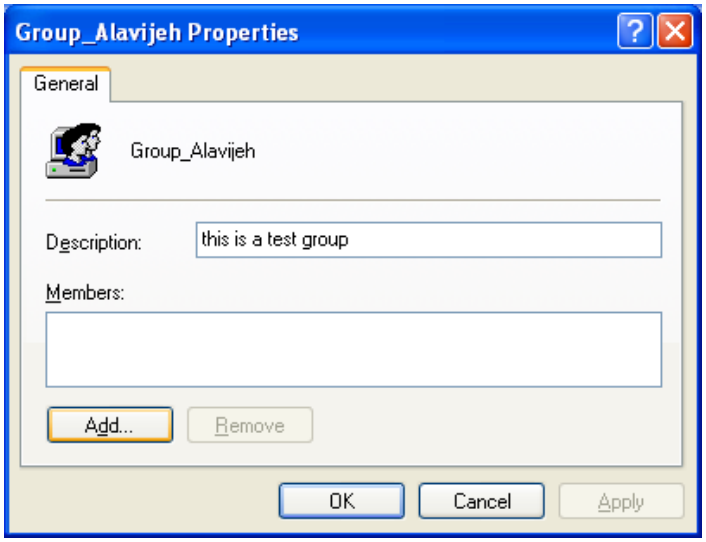
۲- Domain Local Groups: معمولاً برای اعطای مجوز استفاده می شود.

۳- Universal Groups: برای مجوز دادن به کاربران در شبکه هایی که بیش از یک Domain دارند، استفاده می شود.

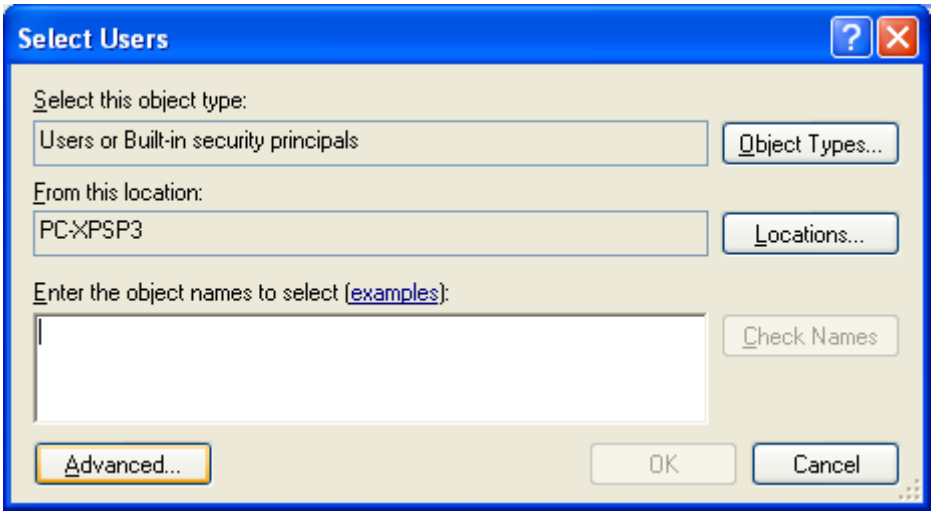
پس از ساخت گروه، نوبت به عضو گیری برای گروه می شود. بدین منظور روی گروه راست کلیک کرده و گزینه Properties را انتخاب کنید.



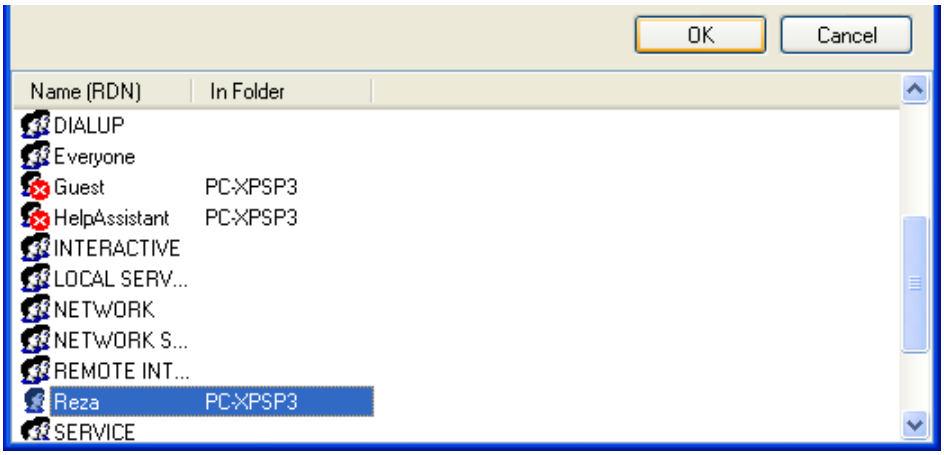
در پنجره باز شده، ابتدا وارد سربرگ Members شده و روی دکمه Add کلیک کنید.



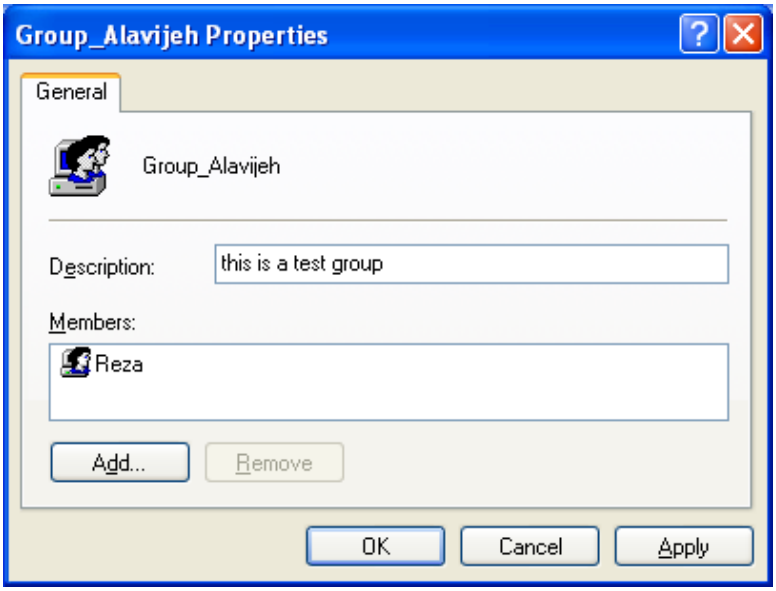
سپس برای انتخاب کاربر یا گروهی خاص برای عضو کردن در این گروه روی دکمه Advanced کلیک کنید.



سپس در صفحه باز شده، روی دکمه Find Now کلیک کرده، کاربران یا گروه های مورد نظر را انتخاب کرده و سپس دو مرتبه OK کنید تا اعضای انتخاب شده عضوی از این گروه شوند. در این مثال ما کاربر Reza را عضو این گروه کرده ایم.



سپس اعضای این گروه را مشاهده خواهید نمود.

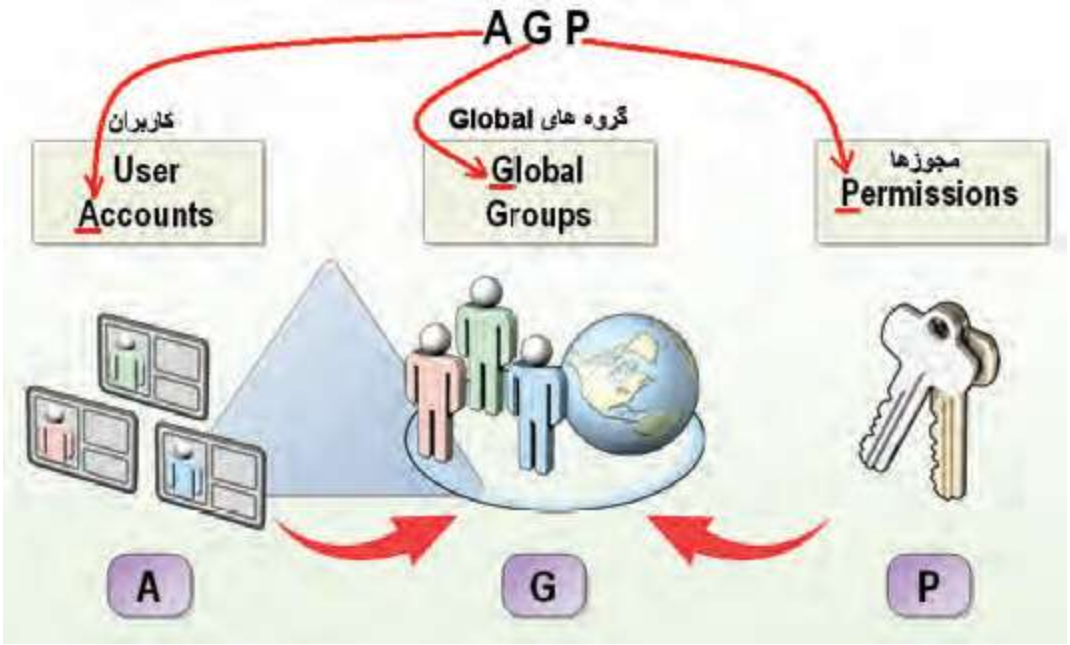


همچنین می توان کاربر یا گروهی خاص را به روشی دیگر عضوی از یک گروه کرد. بدین منظور ابتدا روی کاربر یا گروه مورد نظر راست کلیک کرده، گزینه Properties را انتخاب کرده و سپس وارد سربرگ Member Of شود. در صفحه باز شده، روی دکمه Add کلیک کرده و سپس گروه یا گروه هایی که قصد عضویت در آن را دارید انتخاب نمایید.

۱۶-۴-۱- روش های اعطای مجوز به کاربران

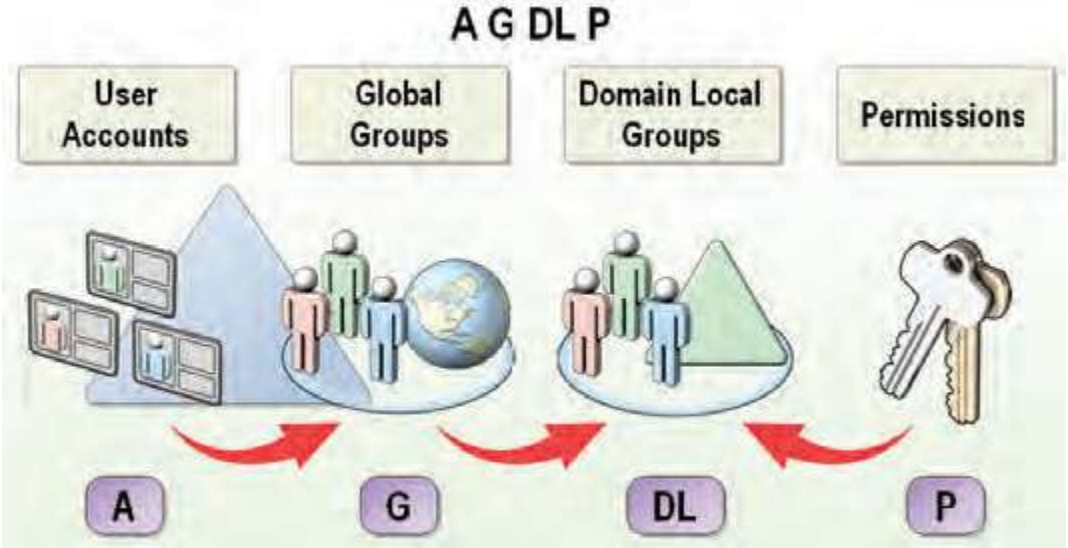
از روش های مختلفی برای اعطای مجوز به کاربران به کمک گروه ها می توان استفاده نمود.

- **روش AGP:** در این روش کاربران (Account ها) را در گروه های مختلف از نوع Global دسته بندی می کنند. این دسته بندی از نظر **نوع کار و محل جغرافیایی کاربران** انجام می شود. سپس مجوز (Permission) لازم به گروه ها اعطا می شود. از این روش در شبکه هایی که تعداد Object ها زیاد نیست می توان استفاده کرد.



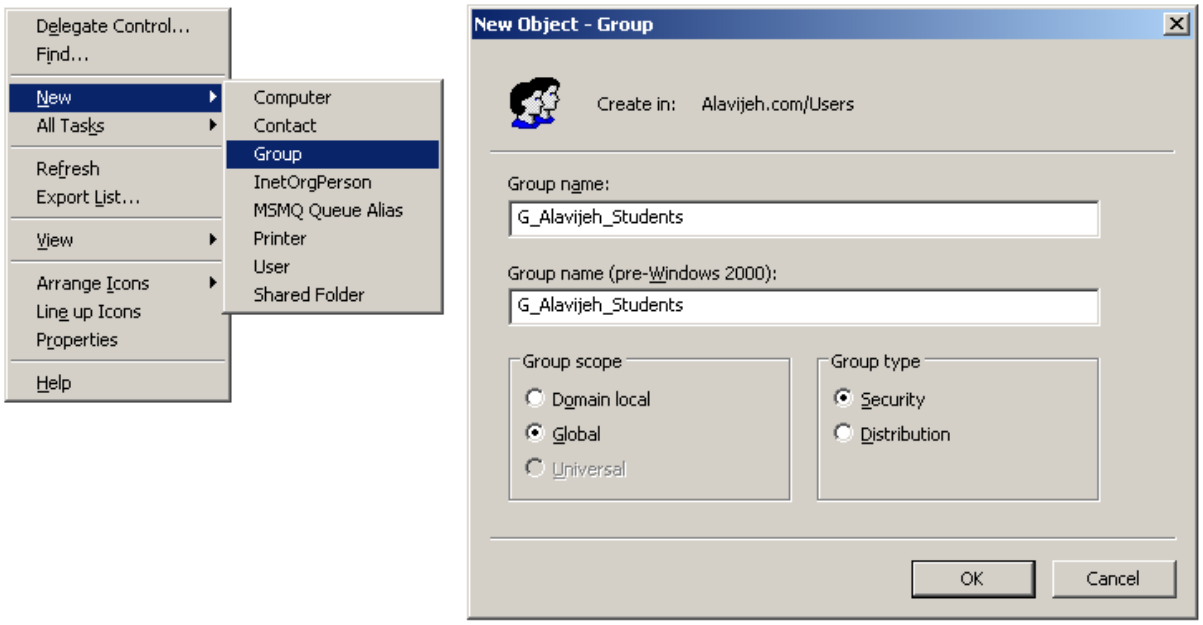
- **روش ADLP:** در این روش کاربران (Account ها) را در گروه های مختلف از نوع Global دسته بندی می کنند. سپس گروه هایی از نوع Local Domain ایجاد کرده و به آنها مجوز (Permission) لازم را اعطا می کنند. حال تمامی گروه های Global که لازم است مجوزهای مربوط را داشته باشند را می توان به عضویت گروه های Local Domain در آورد. از این روش در شبکه هایی که تعداد Object های زیادی دارند و یا شبکه هایی که از چندین Domain تشکیل شده اند، استفاده می شود.

- **روش AGDLP:** در این روش کاربران را در گروه های مختلف از نوع Global دسته بندی می کنند. سپس گروه های از نوع Domain Local ایجاد کرده و به آنها مجوز لازم را اعطا می کنند. حال تمامی گروه های Global که لازم است مجوزهای مربوطه را داشته باشند به عضویت گروه های Domain Local در می آورند. از این روش در شبکه هایی که تعداد Object هایی زیادی دارند و یا شبکه هایی که از چندین دامنه تشکیل شده اند می توان استفاده کرد.

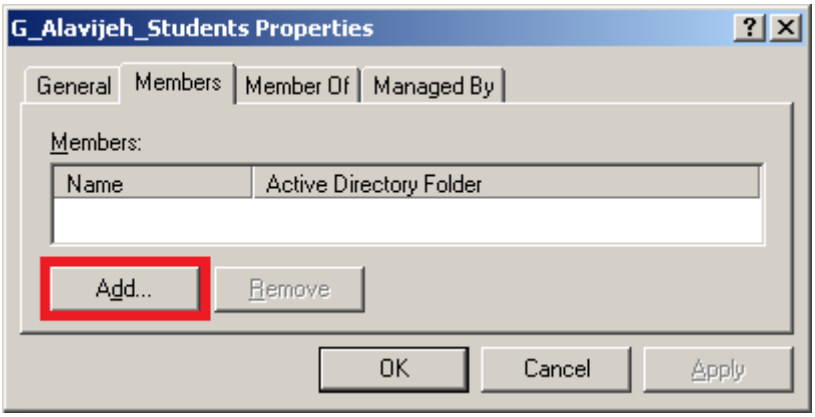


۱۶-۴-۲- پیاده سازی روش های مختلف اعطای مجوز به کاربران

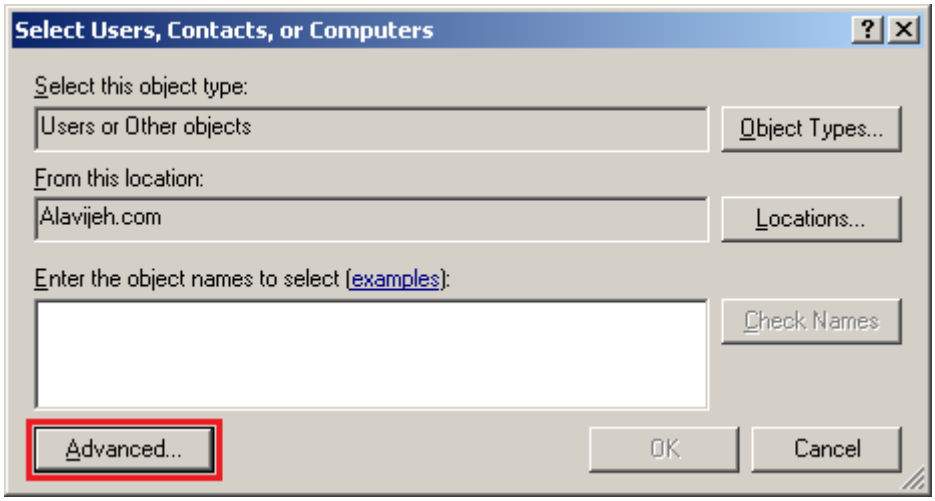
پیاده سازی روش AGP: در این روش ابتدا یک گروه از نوع Global به همان شیوه ای که در مراحل قبل یاد گرفتید، با نام G_Alavijeh_Students ایجاد کنید.



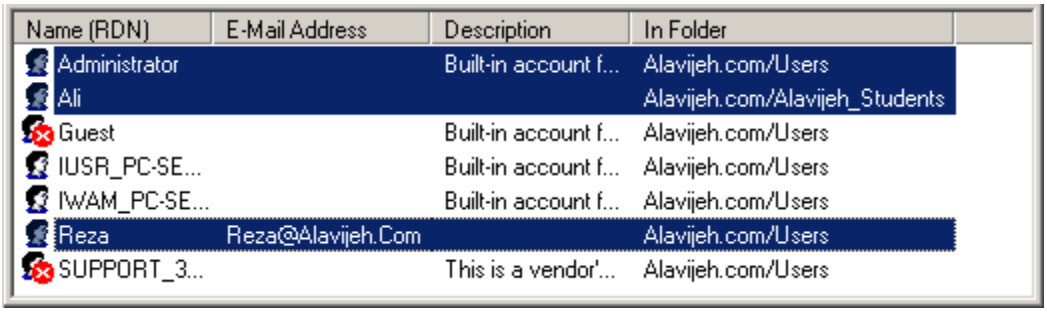
سپس روی این گروه راست کلیک کرده و Properties را انتخاب نمایید. سپس وارد سربرگ Members شوید. در زبانه Members لیست اعضای این گروه را مشاهده کنید.



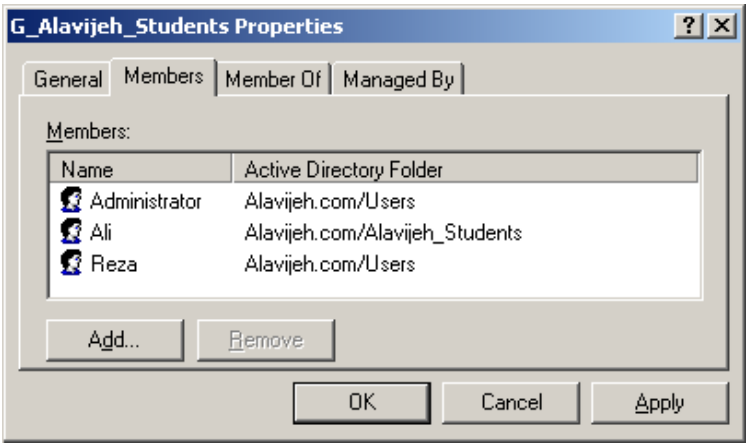
حال بایستی کاربرانی را عضو این گروه نمایید. بدین منظور روی دکمه Add کلیک کنید تا شکل زیر ظاهر شود.



در پنجره فوق می توانید اسامی کاربران را تایپ کرده و به لیست اضافه نمائید و یا برای انتخاب کاربران از لیست روی کلید Advanced کلیک کرده و سپس روی گزینه Find Now کلیک نمائید تا لیستی از کاربران و گروه ها نمایش داده شوند. حال کاربران مورد نظر را به کمک کلیدهای Ctrl و یا Shift انتخاب کرده و به لیست اضافه نمائید.

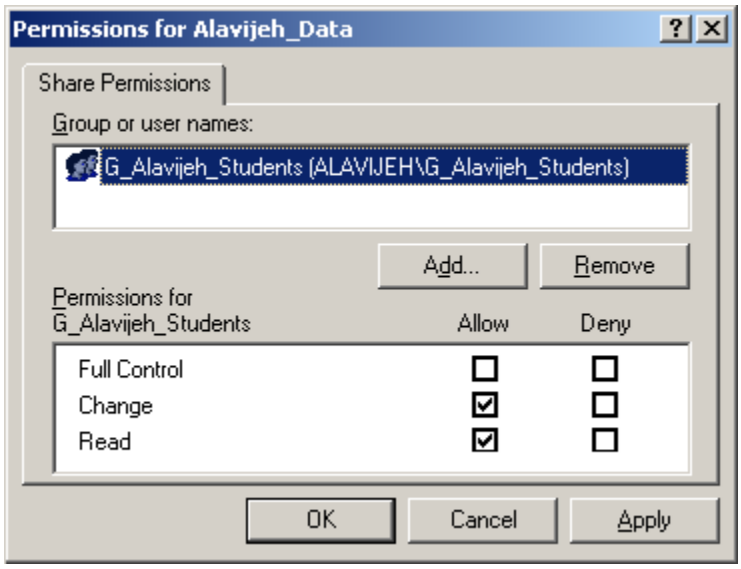


مشاهده خواهید کرد که این کاربران در زبانه Members لیست شده اند. روی گزینه OK کلیک کنید.

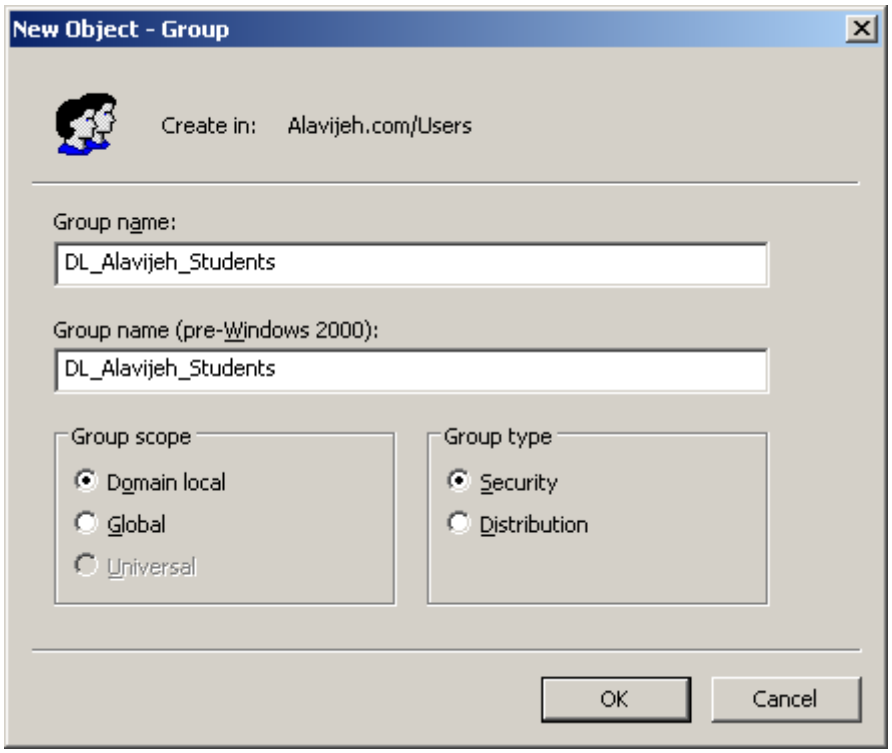


حال در هر جایی که منابع قرار دارند به این گروه مجوز می دهید. به عنوان مثال فرض کنید که یک پوشه به اشتراک گذاشته شده با نام Alavijeh_Data وجود دارد. روی این پوشه کلیک راست کرده و زبانه Sharing And Security را انتخاب کنید. در پنجره ظاهر شده روی دکمه Permissions کلیک کنید تا پنجره انتخاب کاربر گشوده شود.

در این پنجره گروه Every One را حذف کرده و سپس گروه G_Alavijeh_Students را به لیست اضافه کرده و مجوزهای لازم را به آن انتساب دهید.



پیاده سازی روش ADLP: این روش مشابه روش قبلی می باشد با این تفاوت که گروه را با نام DL_Alavijeh_Students ایجاد کرده و نوع آن را Domain Local انتخاب می کنیم. (بقیه مراحل مانند فوق صورت می گیرد.)



پیاده سازی روش AGDLP: در این روش ابتدا یک دسته بندی منطقی برای کاربران در نظر گرفته و سپس گروه های از نوع Global را ایجاد می کنیم و کاربران را براساس آن دسته بندی بـه عضـویت گـروه هـای مختلـف (گـروه هـای از نـوع Global) در می آوریم. سپس یک گروه از نوع Local Domain ایجاد کرده و تمامی گروه هـای از نـوع Global را عضـو ایـن گروه Local Domain می کنیم. در نهایت مجوزهای لازم روی منبع مورد نظر را به گروه Local Domain اعطا می نماییم. به عنوان مثال یک گروه با نام Alavijeh_Local_Users از نوع Local Domain ایجاد نموده و مجوز Print را روی یک چاپگر به اشتراک گذاشته شده به آن اعطا می کنیم. البته بایستی گروه هایی که از نوع Global هستند و آن ها را قـبلاً سـاخته ایـم را عضو گروه Alavijeh_Local_Users (گروهی از نوع Local Domain) کنیم.

۱۶-۵- واحد های سازمانی یا Organizational Unit (OU)

Organizational Unit یا واحد سازمانی (به اختصار OU)، یک نوع پیشرفته و گسترش یافته Group است. گروه ها فقط مـی توانند User و Group را در خود نگهداری کنند؛ اما OU می تواند شـامل هـر نـوع موجـودیتی باشـد، ماننـد: User، Group، Computer، Printer، Organizational Unit و....

البته تفاوت های دیگری نیز بین Organizational Unit و Group وجود دارد. مهمترین تفاوت این است که ما قابلیت تعریـف Group Policy (سیاست گروهی) روی Organizational Unit را داریم، اما امکان تعیـین Group Policy روی Group وجـود ندارد.

در صورتی که با Group Policy آشنایی ندارید، به فصل Group Policy مراجعه فرمایید.

البته فقـط بـه ایـن نکتـه توجـه داشـته باشـید کـه مفهـوم User و Group در تمـامی ویـنـدوز هـا وجـود دارد. امـا مفهـوم Organizational Unit فقط در ویندوز سرور و در Active Directory آن وجود دارد. لذا اگر در کار ویـنـدوز سـرور، تـازه کـار هستید، احتمالا مفهوم Organizational Unit برای شما جدید خواهد بود.

اما به نظر شما مهمترین کاربرد Organizational Unit چیست؟ به نظـر بنـده کـه مهمتـرین کـاربرد Organizational Unit، نگهداری قسمت های منطقی یک سازمان است. فرض کنید که یک شرکت برنامه نویسی راه انـدازی کـرده ایـد. ایـن شـرکت شامل ۲ گروه عملیاتی ۱- برنامه نویسان و ۲- تحلیلگران است. در هر کدام از این گروه ها، چند نفر مشغول کارند. هر کدام از آن ها یک یا چند کامپیوتر دارند و هر گروه نیز یک چاپگر برای خود دارد. یک راه منطقی این است که هر کدام از این مـوارد

را در یک دسته قرار دهیم. از آنجا که گروه قابلیت نگهداری اجزاء شبکه مانند چاپگر و کامپیوتر را ندارد، لذا مجبوریم از واحد قوی تری به نام Organizational Unit استفاده کنیم. لذا هر کدام از این دو گروه را در OUهای جدا قرار می دهیم. از طرف دیگر، قدرت مدیریت عناصر در ویندوز سرور، بسیار قوی تر از ویندوز های غیر سروری است و از طرفی نیز OU فقط در ویندوز سرور وجود دارد.

به عنوان یک مزیت دیگر OU نسبت به گروه، می توان به این مورد اشاره کرد که در ویندوز سرور این قابلیت وجود دارد که مدیریت یک OU را به یک کاربر خاص واگذار (Delegate) کرد. مثلاً یک کاربر خاص را مامور مدیریت این OU کنیم که این کاربر سطوح دسترسی و خط مشی اعضای این OU را تعیین کند.

به طور خلاصه مزایای Organizational Unit (نسبت به گروه) به صورت زیر است:

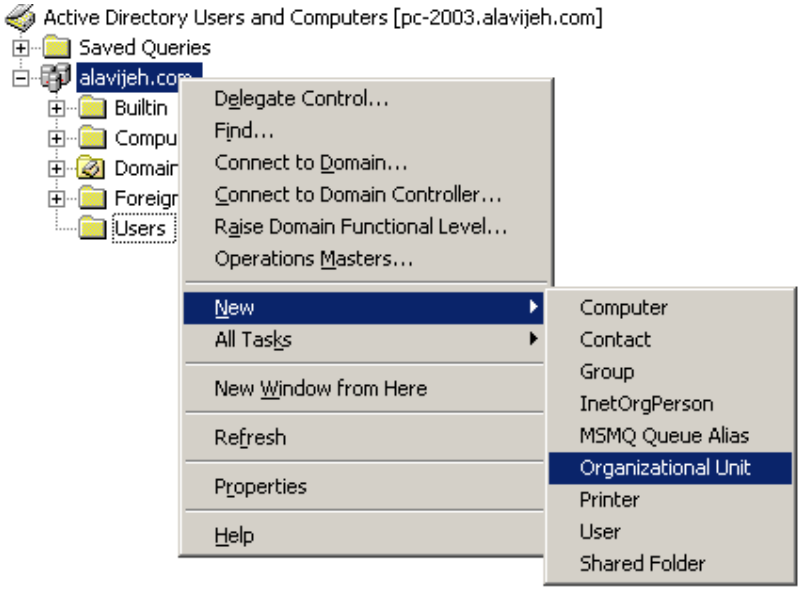
۱. OU می تواند شامل هر نوع موجودیتی باشد، مانند: User، Group، Computer، Printer، Organizational Unit و....
۲. قابلیت تعریف Group Policy (سیاست گروهی) روی Organizational Unit وجود دارد.
۳. OU فقط در ویندوز سرور وجود دارد که ویندوز سرور خیلی قوی تر از ویندوز های غیر سروری است.
۴. قابلیت دسته بندی واحد های منطقی سازمان در آن وجود دارد.
۵. می توان مدیریت یک OU را به یک کاربر خاص واگذار (Delegate) کرد.

۱۶-۶- نحوه ساخت واحد سازمانی

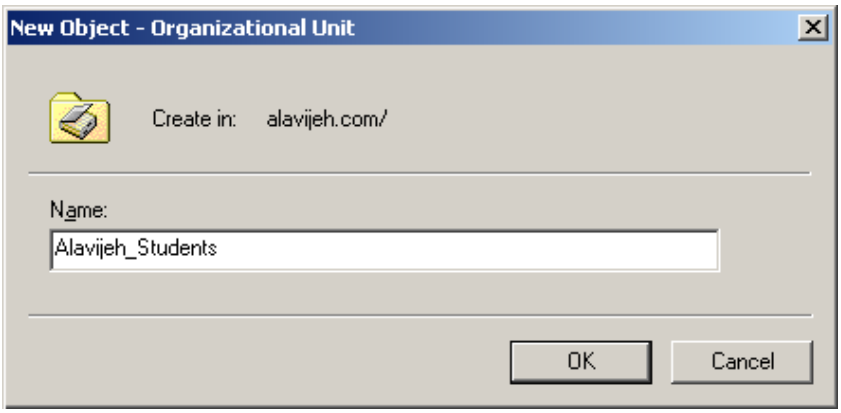
توضیح دادیم که ساخت OU فقط در ویندوز سرور امکان پذیر است. برای ساخت OU، مراحل زیر را طی کنید:

در قسمت Start بر روی Administrative Tools کلیک و سپس گزینه Active Directory Users and Computers را انتخاب نمائید.

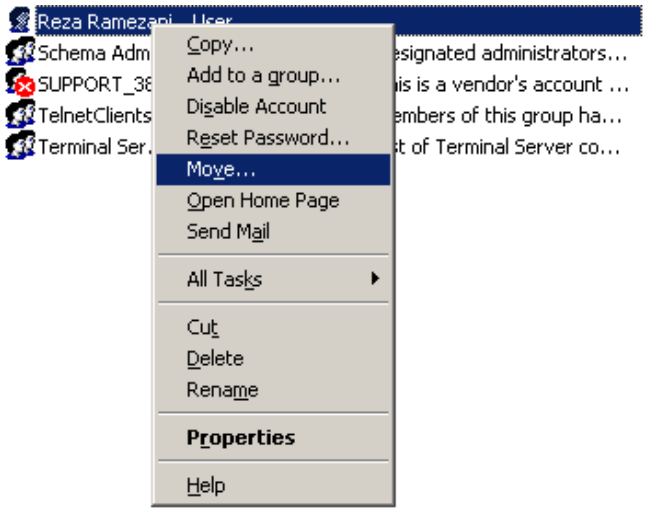
مطابق شکل زیر، روی نام سرور راست کلیک کرده و از منوی New گزینه Organization Unite را انتخاب نمایید.



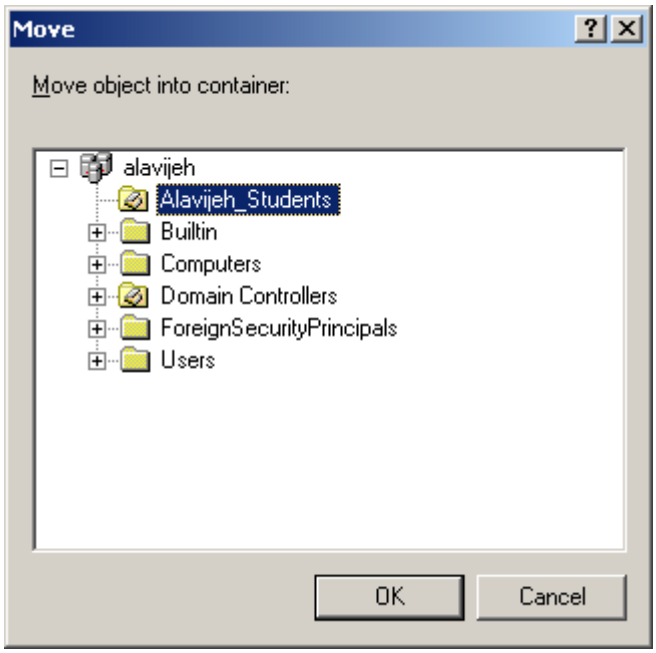
سپس یک نام برای واحد سازمانی خود (مثلاً Alavijeh_Students) وارد نمایید.



در ویندوز سرور ۲۰۰۳، هر کاربری که جدید ساخته شود به صورت پیش فرض در گروه Users قرار می گیرد پس برای اینکه بتوانید User یا Group ایجاد شده را عضو OU جدید کنید، آن را توسط موس داخل OU ساخته شده (در این مثال Alavijeh_Students) بیندازید. برای انتقال کاربر، روی آن راست کلیک کرده، گزینه Move را انتخاب کرده، مقصد را انتخاب نموده تا کاربر به آن انتقال یابد. در صورتیکه کاربری ایجاد نکرده اید بر روی Organization Unit ساخته شده راست کلیک کرده و از آنجا یک کاربر جدید بسازید تا از همان ابتدا عضو آن واحد سازمانی قرار گیرد.



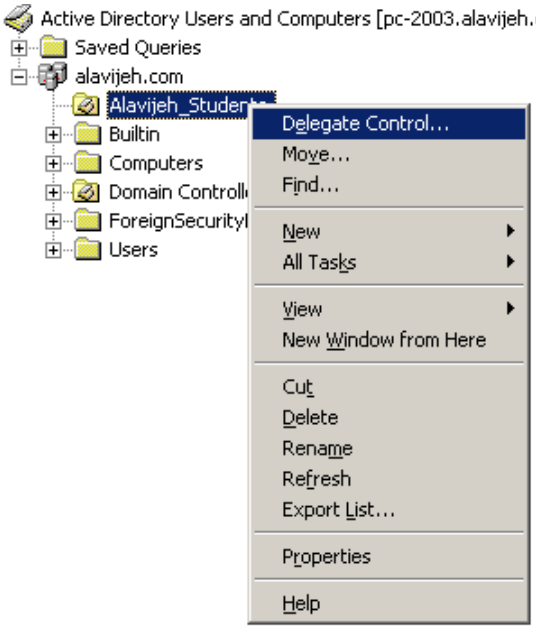
انتخاب مقصد کاربر:



اکنون Organization Unit ساخته شده و اعضای آن نیز مشخص می باشند حال باید برای آنها Group Policy تعریف گردد. برای درک مفهوم Group Policy و آشنایی عملی با آن، به فصل Group Policy مراجعه نمایید.

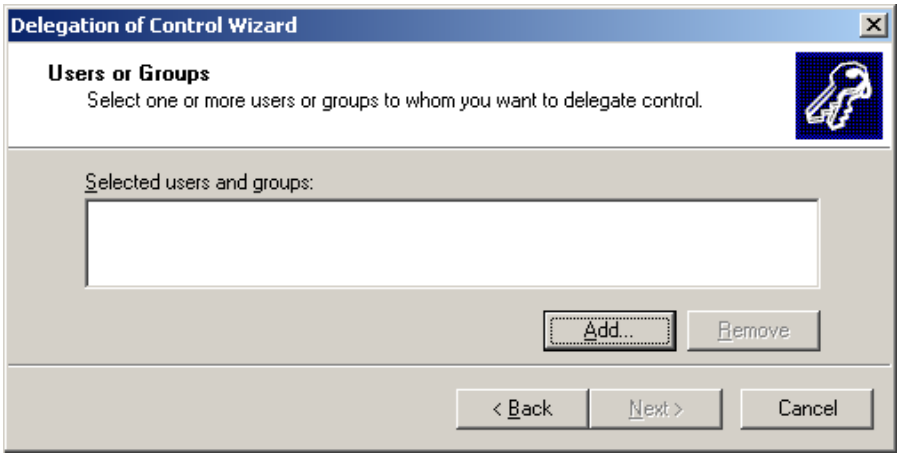
۱۶-۷- واگذاری مدیریت OU

در قسمت فوق اشاره کردیم که یکی از مزایای OU نسبت به Group این است که OU این قابلیت را دارد که می توان مدیریت OU را به یک کاربر واگذار کرد تا این کاربر خاص، خودش مدیریت OU را به عهده بگیرد. بدین منظور بر روی OU ساخته شده راست کلیک کرده و گزینه Delegate Control را انتخاب کنید.

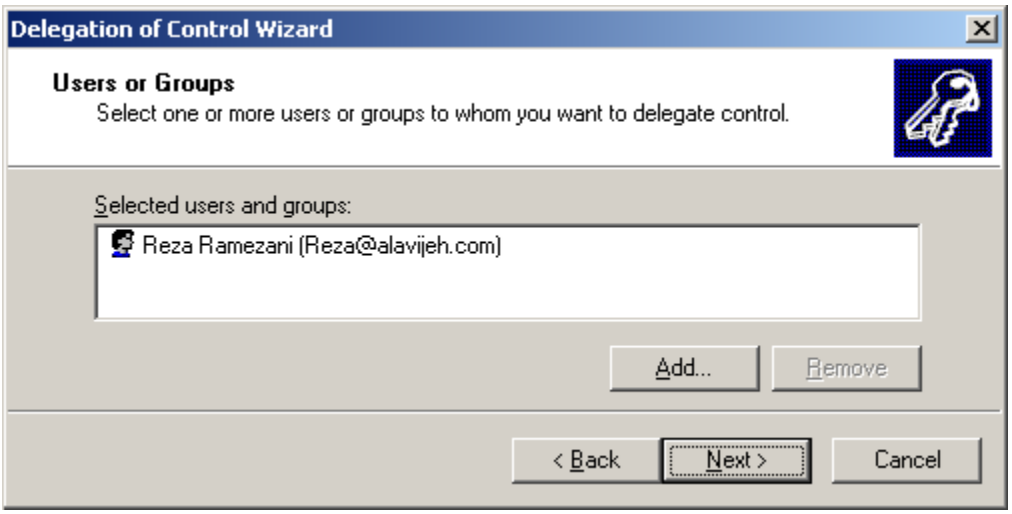


در صفحه خوش آمد گویی، دکمه Next را انتخاب کنید.

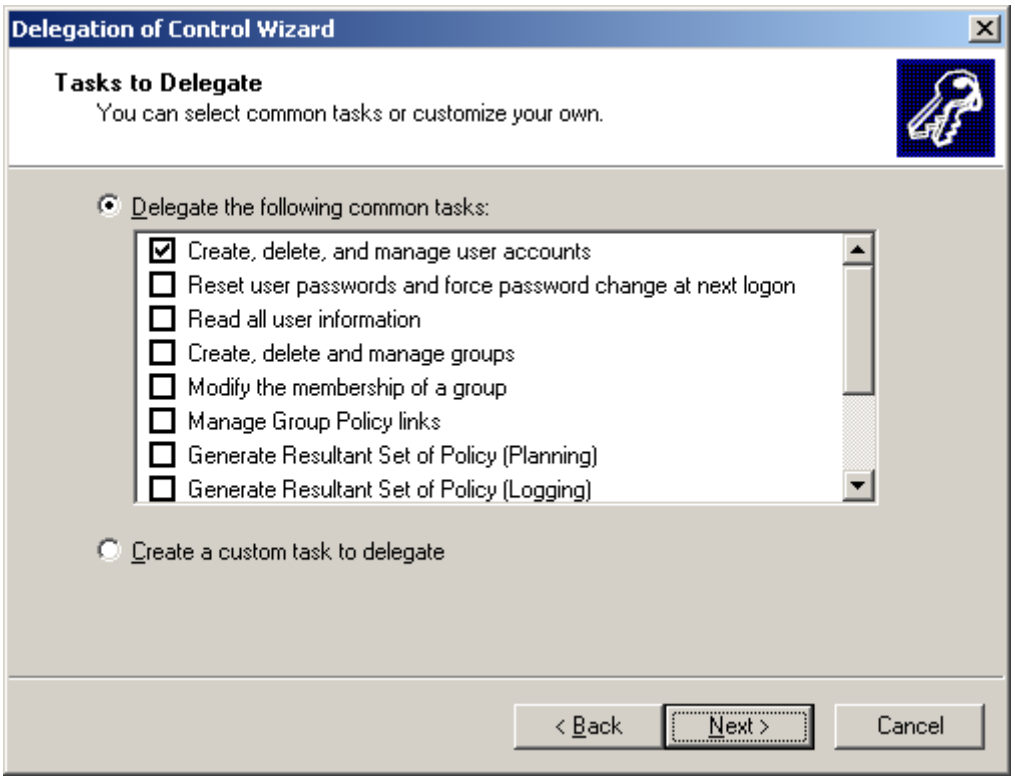
سپس در صفحه باز شده، کاربرانی که می خواهند مدیریت این OU را بر عهده بگیرند انتخاب کنید. بدین منظور روی دکمه Add کلیک کنید.



پس از انتخاب کاربری خاص، این کاربر در لیست مدیران OU قرار می گیرد. سپس روی دکمه Next کلیک کنید.



سپس در صفحه باز شده، سطوح دسترسی و قابلیت های مدیریتی کاربر انتخاب شده را تعیین نمایید. در مثال زیر، ما قابلیت ساخت و حذف اعضای OU را به کاربر داده ایم. سپس روی Next کلیک کنید.



در پایان بر روی دکمه Finish کلیک کنید. بدین ترتیب کاربر انتخاب شده قابلیت مدیریت OU ساخته شده را دارد.

فصل ۱۷

DNS Server

۱۷-۱- DNS (Domain Name Server)

DNS، ابزاری جهت تبدیل Host Name (نام کامپیوتر) به IP Address مربوطه می باشد.

هر کامپیوتر در شبکه یک Host نامیده می شود و علاوه بر IP Address دارای یک عنوان مشخص کننده دیگر به نام Host Name می باشد. یک کامپیوتر برای بدست آوردن IP Address متناظر با Host Name، از کامپیوتری در شبکه به نام DNS Server کمک می گیرد. DNS Server، حاوی نام و IP Address کامپیوتر مورد نظر می باشد که پس از مقایسه درخواست با اطلاعات موجود در Database خود، IP Address مورد نظر را بر میگرداند.

جهت استفاده از DNS به اجزای زیر نیازمند خواهیم بود:

۱. DNS Client یا درخواست کننده IP Address
۲. DNS Server که حاوی اطلاعات مربوط به نام Host و IP Address، منابع موجود و نوع آن در شبکه می باشد. که به این بانک اطلاعاتی، Resource Record یا به اختصار RR گفته می شود.

لازم به ذکر است که DNS Server های موجود در اینترنت، جهت تبدیل نام به IP Address در شبکه اینترنت استفاده می شود.

۱۷-۲- تاریخچه DNS

DNS، زمانی که اینترنت تا به این اندازه گسترش پیدا نکرده بود و صرفاً در حد و اندازه یک شبکه کوچک بود، استفاده می گردید. در آن زمان، اسامی کامپیوتر های میزبان (سرور ها) به صورت دستی در فایلی با نام HOSTS درج می گردید (برای پیدا کردن این فایل در ویندوز، به آدرس C:\Windows\System32\drivers\etc مراجعه نمایید). فایل فوق بر روی یک سرویس دهنده مرکزی قرار می گرفت. هر سایت و یا کامپیوتر که نیازمند ترجمه اسامی کامپیوتر های میزبان بود، می بایست از فایل فوق استفاده می نمود. همزمان با گسترش اینترنت و افزایش تعداد کامپیوتر های میزبان، حجم فایل فوق نیز افزایش و امکان استفاده از آن با مشکل مواجه گردید (افزایش ترافیک شبکه). با توجه به مسائل فوق، در سال ۱۹۸۴ تکنولوژی DNS معرفی گردید.

۱۷-۳- پروتکل DNS

DNS، یک "بانک اطلاعاتی توزیع شده" است که بر روی ماشین های متعددی مستقر می شود (مشابه ریشه های یک درخت که از ریشه اصلی انشعاب می شوند). در صورت استفاده از ویندوز ۲۰۰۳ و اکتیو دایرکتوری، قطعا از DNS به منظور ترجمه اسامی کامپیوتر ها به آدرس های IP، استفاده می شود. شرکت مایکروسافت ابتدا نسخه اختصاصی سرویس دهنده DNS خود را با نام WINS (Windows Internet Name Service) طراحی و پیاده سازی نمود. و سپس به علت قدیمی بودن آن به سمت DNS حرکت کند. DNS مسئولیت حل مشکل اسامی کامپیوتر ها (ترجمه نام به آدرس) در یک شبکه و مسائل مرتبط

با برنامه های Winsock (برنامه های سوکت که در ویندوز نوشته می شوند و در آن برای آدرس دهی یک کامپیوتر از آدرس IP کامپیوتر استفاده می شود) را بر عهده دارد.

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

کامپیوتر ها جهت کار با اعداد (خصوصا IP) دارای مسائل و مشکلات بسیار ناچیزی می باشند. در صورتی که انسان در این رابطه دارای مشکلات خاص خود است. به هرحال به خاطر سپردن اسامی کامپیوتر ها به مراتب راحت تر از بخاطر سپردن اعداد (کد) است. از آنجایی که برنامه های Winsock نیازمند آگاهی از نام کامپیوتر یا Host Name نمی باشند، می توان با رعایت تمامی مسائل جانبی از روش فوق برای ترجمه اسامی استفاده کرد. فرآیند فوق را ترجمه اسامی (Hostname Resolution) می گویند.

DNS Namespace -۴-۱۷

DNS از یک ساختار سلسله مراتبی برای سیستم نام گذاری خود استفاده می نماید. با توجه به ماهیت سلسله مراتبی بودن ساختار فوق، چندین کامپیوتر می توانند دارای اسامی یکسان بر روی شاخه های مختلف بوده و هیچگونه نگرانی از عدم ارسال پیام ها وجود نخواهد داشت. ویژگی فوق درست نقطه مخالف سیستم نامگذاری NetBIOS است. در مدل NetBIOS قادر به انتخاب دو نام یکسان برای دو کامپیوتر نخواهیم نبود.

NetBIOS یک پروتکل قدیمی می باشد که برای برقراری ارتباط میان کامپیوتر ها توسط شرکت IBM ایجاد شد (پروتکل ها مجموعه قوانین و مقرراتی هستند که برای انجام یک فرآیند خاص در شبکه های کامپیوتری تعریف می شوند). قابلیتی که این پروتکل ایجاد می کند، این است که، امکان دیدن نام کامپیوتر هایی که در یک گروه کاری (Workgroup) قرار دارند را فراهم می کند.

بالاترین سطح در DNS با نام Root Domain (یا Hint Root) نامیده شده و اغلب به صورت یک "." و یا یک فضای خالی "" نشان داده می شود. بلافاصله پس از ریشه با اسامی موجود در دامنه بالاترین سطح (Top Level) برخورد خواهیم کرد. مثلاً دامنه های .Com، .net، org. و edu.

اینترنت به چندین ناحیه سطح بالا (Top-Level Domain) که هر کدام تعداد زیادی کامپیوتر را در بر می گیرد، تقسیم می شود. هر ناحیه به چندین زیر ناحیه (Sub Domain) و آنها نیز به نوبه خود به زیر ناحیه های کوچکتر تقسیم می شوند. ناحیه هایی که زیر ناحیه ندارند "برگ" نامیده می شوند.

ناحیه های سطح بالا (Top Level) دو گونه اند: عمومی و کشورها.

ناحیه های عمومی مانند:

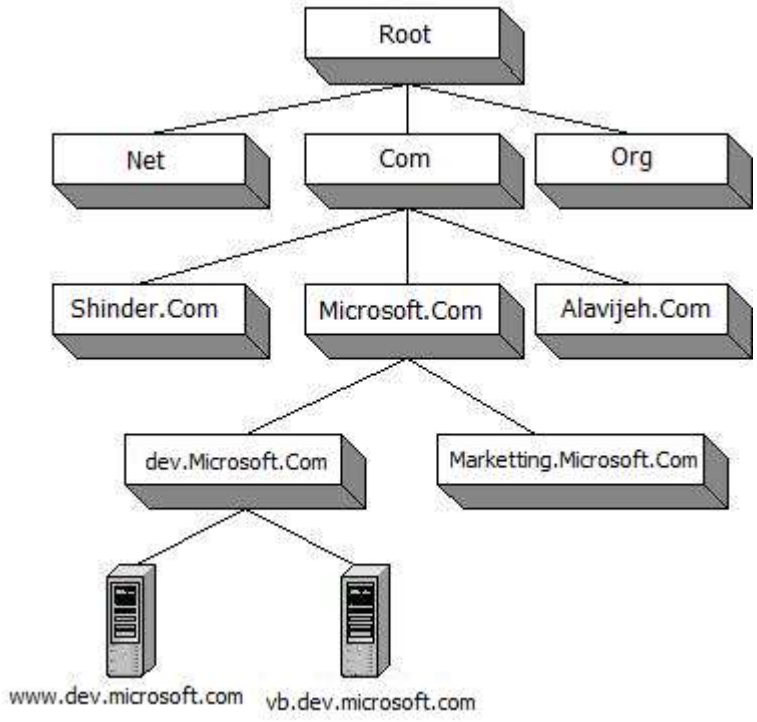
- Com (مخفف Commercial، تجاری)
- Edu (مخفف Educational، مؤسسات آموزشی)
- Net (مخفف Network Provider، شرکتهای خدمات شبکه و اینترنت) و غیره...

ناحیه های کشورها مانند:

- ir (کشور ایران)
- de (کشور آلمان)
- ja (کشور ژاپن)

سازمانهایی که تمایل به داشتن یک وب سایت بر روی اینترنت دارند، می بایست یک دامنه را که به عنوان عضوی از اسامی حوزه Top Level می باشد را برای خود اختیار نماید. هر یک از حوزه های سطح بالا دارای کاربردهای خاصی می باشند. مثلاً سازمان های اقتصادی در حوزه .Com و موسسات آموزشی در حوزه .Edu و... دامنه خود را ثبت خواهند نمود.

شکل زیر ساختار سلسله مراتبی DNS را نشان می دهد.



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

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

مشخصات دامنه و اسم Host

هر کامپیوتر در DNS به عنوان عضوی از یک دامنه در نظر گرفته می شود. به منظور شناخت و ضرورت استفاده از ساختار سلسله مراتبی به همراه DNS، لازم است با FQDN با جزئیات بیشتری آشنا شویم.

۱۷-۴-۱- معرفی Fully Qualified Domain Names (FQDN)

یک FQDN، محل یک کامپیوتر خاص را در DNS مشخص خواهد نمود. با استفاده از FQDN می توان به سادگی محل کامپیوتر در دامنه مربوطه را مشخص و به آن دستیابی نمود. FQDN یک نام ترکیبی است که در آن **نام ماشین** (Host) و **نام دامنه** مربوطه با یکدیگر ترکیب شده اند (بحثی شبیه آدرس شبکه و آدرس کامپیوتر در شبکه در مبحث آدرس IP). مثلاً اگر شرکتی با نام Shiraziha در حوزه سطح دوم دامنه خود را ثبت نماید (Shiraziha.Com) در صورتی که سرویس دهنده وب بر روی Shiraziha.Com اجراء گردد، می توان آن را www نامید (www نام Host ماشین مربوطه است و شناسه خدماتی

نیست) کاربران با استفاده از www.Shiraziha.Com به آن دستیابی پیدا نمایند. یک نام FQDN از دو عنصر اساسی تشکیل شده است:

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

هر Lable توسط نقطه از یکدیگر جدا خواهند شد. هر Lable می تواند حداکثر دارای ۶۳ بایت باشد (طول هر Lable بر حسب بایت مشخص شده است نه بر حسب طول رشته؛ علت این است که DNS در ویندوز ۲۰۰۳ از کاراکتر های UTF-8 استفاده می نماید نه کاراکتر های اسکی) طول FQDN باید حداکثر ۲۵۵ بایت باشد.

همانطوری که در شکل زیر مشاهده می کنید، تمامی اسامی اینترنتی به یک نقطه ختم می شوند. البته لازم به توضیح است که کاربران اینترنتی معمولاً این نقطه را در انتهای اسامی اینترنتی وارد نمی کنند و این نقطه به صورت اتوماتیک به اسامی اضافه می شود.

این قسمت از اسامی اینترنتی با نام Root Level (سطح ریشه) شناخته می شود پس می توان نتیجه گرفت که آخرین نقطه در اسامی اینترنتی بخشی از آن اسم نیز می باشد (برخلاف سایر نقطه ها که به عنوان جدا کننده مورد استفاده قرار می گیرند).

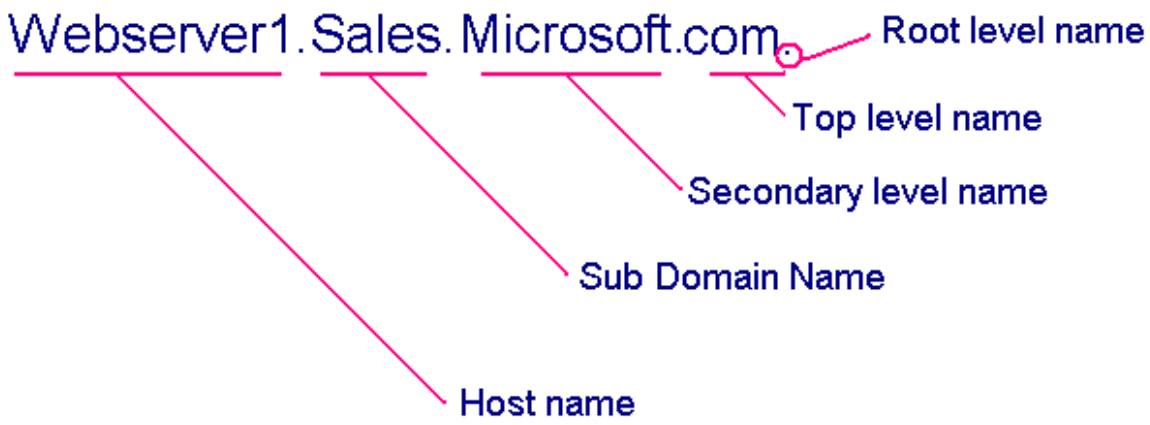
قسمت دوم از سمت راست این اسامی معمولاً اسامی دو یا سه کاراکتری هستند که بیانگر **نوع فعالیت** Domain و یا **محل جغرافیایی** آن Domain می باشند. به عنوان مثال .Com بیانگر فعالیت های تجارتی، .ir بیانگر کشور ایران، .Edu بیانگر فعالیت های آموزشی، .Ca بیانگر کشور کانادا و... می باشند. به اسامی مربوط به این سطح اسامی Top level (سطح بالا) گفته می شود.

قسمت بعد در اسامی اینترنتی مربوط به اسامی شرکت ها و اشخاص و... می باشد. این اسامی به وسیله اشخاص و یا شرکت ها اجاره می شوند. شرکت های خاصی این اسامی را اجاره می دهند. به عنوان مثال Microsoft یا Alavijeh-uast اسامی مربوط به این سطح می باشد که به آن ها اسامی Secondary (ثانویه) گفته می شود. نظارت بر اسامی اینترنتی و تشخیص آن ها به عهده شرکت Internic می باشد.

ایجاد Sub Domainها (زیر دامنه ها) به شرکت های مربوطه واگذار می شود (خود فرد یا شرکت صاحب دامنه). به عنوان مثال در داخل Microsoft، یک زیر دامنه به نام Training ایجاد شده است. ایجاد و نگهداری این زیر دامنه به عهده شرکت مایکروسافت می باشد: Training.Microsoft.Com

اسامی Hostها یا Sub Domain ها از پائین ساختار درختی شروع شده و به ریشه ختم می گردد.

به عنوان مثال در شکل زیر یک Host با نام www وجود دارد که FQDN آن www.Microsoft.com می باشد. یا یک Host دیگری به نام WebServer وجود دارد که FQDN آن WebServer.Training.Microsoft.com. می باشد. شکل زیر قسمت های مختلف این اسم را تشریح می کند.



۱۷-۴-۲- استفاده از نام یکسان دامنه برای منابع اینترنت و اینترانت

به منظور حفاظت ناحیه (Zone) های DNS از دستیابی غیر مجاز، نباید هیچ گونه اطلاعاتی در رابطه با منابع داخلی بر روی سرویس دهنده DNS نگهداری نمود. بنابراین می بایست برای یک دامنه از دو Zone متفاوت استفاده نمود. یکی از Zone ها، منابع داخلی را دنبال می کند و Zone دیگر، مسئولیت پاسخگوئی به منابعی است که بر روی اینترنت قرار دارند. عملیات فوق قطعا حجم وظایف مدیریت سایت را افزایش خواهد داد.

۱۷-۴-۳- پیاده سازی نام یکسان برای منابع داخلی و خارجی

یکی دیگر از عملیات پیاده سازی دامنه های یکسان برای منابع داخلی و خارجی، Mirror نمودن منابع خارجی به صورت داخلی است. مثلاً فرض نمائید که Test.Com نام انتخاب شده برای دستیابی به منابع داخلی (اینترانت) و منابع خارجی (اینترنت) است. می خواهیم از اسامی یکسان برای سرویس دهندگان استفاده نماییم. اگر درخواستی برای www.Test.Com صورت پذیرد، مسئله به کامپیوتری ختم خواهد شد که قصد داریم برای کاربران اینترنت قابل دستیابی باشد. در وضعیت هایی که نخواهیم کاربران اینترنت قادر به دستیابی به اطلاعات شخصی و داخلی سازمان باشند. حل مشکل فوق، Mirror نمودن منابع اینترنت به صورت داخلی است و ایجاد یک Zone در DNS برای دستیابی کاربران به منابع داخلی ضروری خواهد بود. زمانیکه کاربری درخواست www.Test.Com را صادر نماید، در ابتدا مسئله نام از طریق سرویس دهنده داخلی DNS برطرف خواهد شد که شامل Zone داخلی مربوطه است. زمانی که یک کاربر اینترنت قصد دستیابی به www.Test.Com را داشته باشد، درخواست وی به **سرویس دهنده اینترنت** DNS ارسال خواهد شد؛ که در چنین حالتی آدرس IP سرویس دهنده خارجی DNS برگردانده خواهد شد.

۱۷-۴-۴- استفاده از اسامی متفاوت برای دامنه ها ی اینترنت و اینترانت

در مدل فوق نیازی به نگهداری Zone های متفاوت برای هر یک از آنها نبوده و هریک از آنها دارای یک نام مجزا و اختصاصی مربوط به خود خواهند بود. مثلاً می توان نام **اینترنتی** حوزه را Test.Com و نام اینترانتی آن را Test.Local قرار داد.
برای نامگذاری هر یک از زیر دامنه ها می توان اسامی انتخابی را براساس نوع فعالیت و یا حوزه جغرافیایی انتخاب نمود.

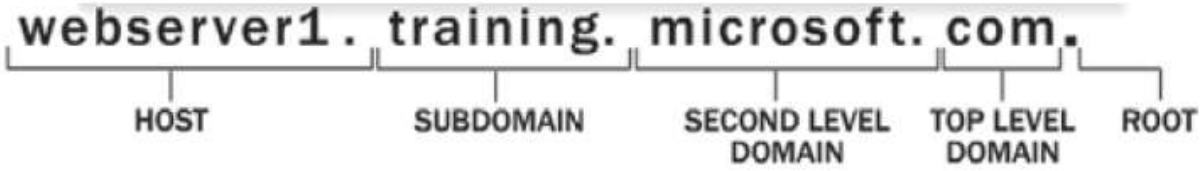
۱۷-۵- اجزاء DNS

یک DNS Server دارای اجزاء زیر می باشد:

۱- **Name Server**: به DNS Server، Name Server نیز اطلاق می شود و یک سرور ۲۰۰۳ است (در این جزوه) که سرویس DNS روی آن نصب گردیده است.

۲- **Zone**: یک DNS Server اطلاعات مربوط به Domainهای مختلف را می تواند نگهداری کرده و به کاربران در ارتباط با آنها سرویس دهد. برای نگهداری اطلاعات Domain در DNS از Zone استفاده می شود. به عبارت دیگر بانک اطلاعاتی DNS سرور همان Zone می باشد.

در FQDN (شکل زیر)، به هر کدام از گزینه های Secondary Level مثل Microsoft یا Yahoo، یک Domain گفته می شود. زمانی که این Domain ها را در DNS می خواهیم پیاده سازی کنیم، باید آنها را با Zone ایجاد نماییم. بنابر این در شکل و نمودارها از واژه Domain و در عمل از Zone استفاده می شود.



Zone ها به دو دسته کلی تقسیم می شوند.

- **Forward Lookup Zones**: Zone هایی هستند که برای تبدیل اسم به IP استفاده می شوند.
- **Revers Lookup Zones**: Zone هایی هستند که برای تبدیل IP به اسم استفاده می شوند.

۳- **Resource Records**: در یک Zone اطلاعات مربوط به یک Domain نگهداری می شود. این اطلاعات به صورت رکورد ثبت و نگهداری می شوند. به عنوان مثال اسم و IP یک Host در یک رکورد از نوع Host قرار می گیرند. رکورد از نوع Host بیشترین استفاده را در DNS دارا می باشد، ولی از انواع رکورد ها در یک Zone می توان استفاده نمود که تعدادی از این نوع رکورد ها عبارتند از:

- **Host Record**: از این رکورد به منظور تبدیل اسم به IP استفاده می شود.
- **Point Record**: از این رکورد به منظور تبدیل IP به اسم استفاده می شود.
- **SRV Record**: از این رکورد به منظور معرفی سرویس دهنده هایی که سرویس های خاص را ارائه می کنند، استفاده می شود.
- **NS Record**: از این رکورد برای معرفی Name server (DNS) استفاده می شود.
- **SOA Record**: از این رکورد برای معرفی اطلاعاتی در ارتباط با یک Zone استفاده می شود.
- **Alias Record**: از این رکورد برای استفاده از اسم مستعار بجای FQDN استفاده می شود.

۱۷-۶- ناحیه ها یا Zone ها (Zones of Authority)

DNS دارای ساختاری است که از آن برای گروه بندی و دنبال نمودن ماشین مربوطه، براساس نام Host در شبکه استفاده خواهد شد. به منظور فعال نمودن DNS در جهت تامین خواسته ای مورد نظر، می بایست روشی جهت ذخیره نمودن اطلاعات در DNS وجود داشته باشد. اطلاعات واقعی در رابطه با دامنه ها در فایلی با نام Zone Database ذخیره می گردد. این نوع فایل ها، فایل های فیزیکی بوده که بر روی سرویس دهنده DNS ذخیره خواهند شد. یعنی برای نگهداری اطلاعات Domain در DNS از Zone استفاده می شود. به عبارت دیگر بانک اطلاعاتی DNS Server همان Zone می باشد. به هر کدام از گزینه های سطح دوم FQDN (مانند Microsoft در www.Microsoft.Com) یک Domain گفته می شود. زمانی که این Domainها را در DNS می خواهیم پیاده سازی کنیم، باید آن ها را با Zone ایجاد کرد. بنابر این در شکل ها و نمودار ها از واژه Domain و در عمل از Zone استفاده می شود. آدرس محل قرار گیری فایل های فوق ./systemroot%\system32\dns خواهد بود. Zone های استاندارد به دو نوع عمده تقسیم می شوند:

- Forward Lookup Zone
- Reverse Lookup Zone

۱۷-۶-۱- Forward Lookup Zone

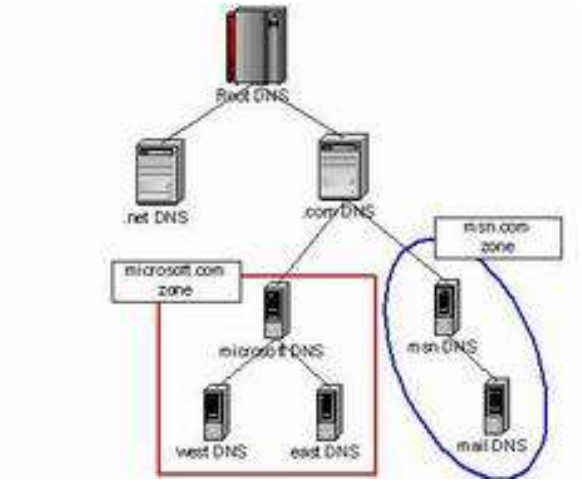
از این نوع Zone برای ایجاد مکانیزمی برای ترجمه اسامی Hostname به آدرس IP برای سرویس گیرندگان DNS استفاده می گردد. Zone ها دارای اطلاعاتی هستند که به صورت رکورد های خاص در بانک اطلاعاتی مربوطه ذخیره خواهند شد. این نوع رکورد ها را رکورد های منبع یا Resource Record می گویند. رکورد های فوق اطلاعات مورد نیاز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

۱۷-۶-۲- Reverse Lookup Zones

Zone های از نوع Forward امکان ترجمه نام یک کامپیوتر به یک IP را فراهم می نمایند. یک Reverse Lookup این امکان را به سرویس گیرندگان خواهد داد که عملیات مخالف عملیات گفته شده را انجام دهند: ترجمه یک آدرس IP به یک نام.

۱۷-۶-۳- تفاوت بین Domain و Zone

Zone ها با دامنه ها (Domain) یکسان نبوده و یک Zone می تواند شامل رکورد هایی در رابطه با چندین دامنه باشد. یعنی می تواند اطلاعات تبدیل آدرس چندین دامنه را در یک Zone قرار دارد، اما بهتر است که همیشه هر Zone فقط اطلاعات یک دامنه را نگهداری کند. مثلاً فرض کنید، دامنه www.Microsoft.Com دارای دو زیر دامنه با نام East و West باشد. (West.Microsoft.Com , East.Microsoft.Com). مایکروسافت دارای دامنه اختصاصی msn.Com بوده که خود شامل دارای یک زیر دامنه با نام mail.Microsoft.Com است.



دامنه های همجوار و غیر هم جوار در شکل فوق نشان داده شده است. دامنه های همجوار همدیگر را حس خواهند کرد (برای یکدیگر ملموس خواهند بود). در رابطه با مثال فوق دامنه های موجود در Microsoft.Com، همجوار و دامنه های Msn.Com و Microsoft.Com غیر هم جوار هستند.

Zone، بخش خاصی از فضای نام است که دارای Resource Record منحصر به فرد می باشد.

۱۷-۶-۴- انواع Zone

۱. **Primary Zone**: که Zone اصلی می باشد.
۲. **Secondary Zone**: که یک کپی از Primary Zone می باشد.
۳. **Stub Zone**: شامل بخش های خاصی از Record ها (بخش خاصی از Primary Zone) می باشد.

۱۷-۶-۵- ویژگی های یک Zone

هر ناحیه (Zone)، خواه ناحیه ای سطح بالا یا ناحیه ای سطح پایین (جزء دامنه های بالاتر) باشد، دارای تعدادی رکورد منبع (Resource Record) است.

برای یک کامپیوتر متداول ترین رکورد منبع، **آدرس IP** (رکورد نوع A) آن است.

هر رکورد منبع پنج بخش دارد:

Domain_Name – Time_To_Live – Class – Type – Value

- **(Domain_Name)** نام ناحیه ای است که این رکورد متعلق به آن است.
- **(Time_To_Live)** دوام و اعتبار رکورد را (بر اساس واحد زمان) مشخص می کند.
- **(Class)** برای اطلاعتت اینترنتی این فیلد همیشه IN است.
- **(Type)** نوع رکورد منبع را مشخص می کند.
- **(Value)** این فیلد می تواند یک عدد، نام ناحیه یا یک رشته متنی باشد.

مهمترین انواع (Type) رکوردهای منبع:

نوع	مفهوم	مقدار
SOA	Start Of Authority	پارامتر های منطقه
A	IP Address Of A Host	عدد صحیح ۳۲ بیتی
MX	Mail Exchange	تقدم دریافت ایمیل
NS	Name Server	نام سرویس دهنده ناحیه
CNAME	Canonical Name	نام ناحیه
PTR	Pointer	نام مستعار برای آدرس IP
HINFO	Host Description	مشخصات CPU و سیستم عامل
TXT	Text	متن تفسیر نشده

از نظر تئوری، برای نگهداری تمام اطلاعات DNS و پاسخ دادن به درخواست ها، یک سرویس دهنده DNS کافیست. اما در عمل، بار کاری چنین کامپیوتری آنقدر سنگین خواهد شد که عملاً آن را بلا استفاده می کند.

برای اجتناب از چنین وضعیتی، فضای نام DNS به چندین منطقه (Zone) با مرزهای مشخص و غیر مشترک تقسیم می شود.

وقتی یک تبدیل کننده می خواهد آدرس ناحیه ای را بداند، ابتدا درخواست خود را به سرویس دهنده های نام محلی خود می دهد.

اگر این ناحیه در محدوده قانونی سرویس دهنده نام مزبور بود، سرویس دهنده نام رکورد های منبع معتبر را به آن بر می گرداند.

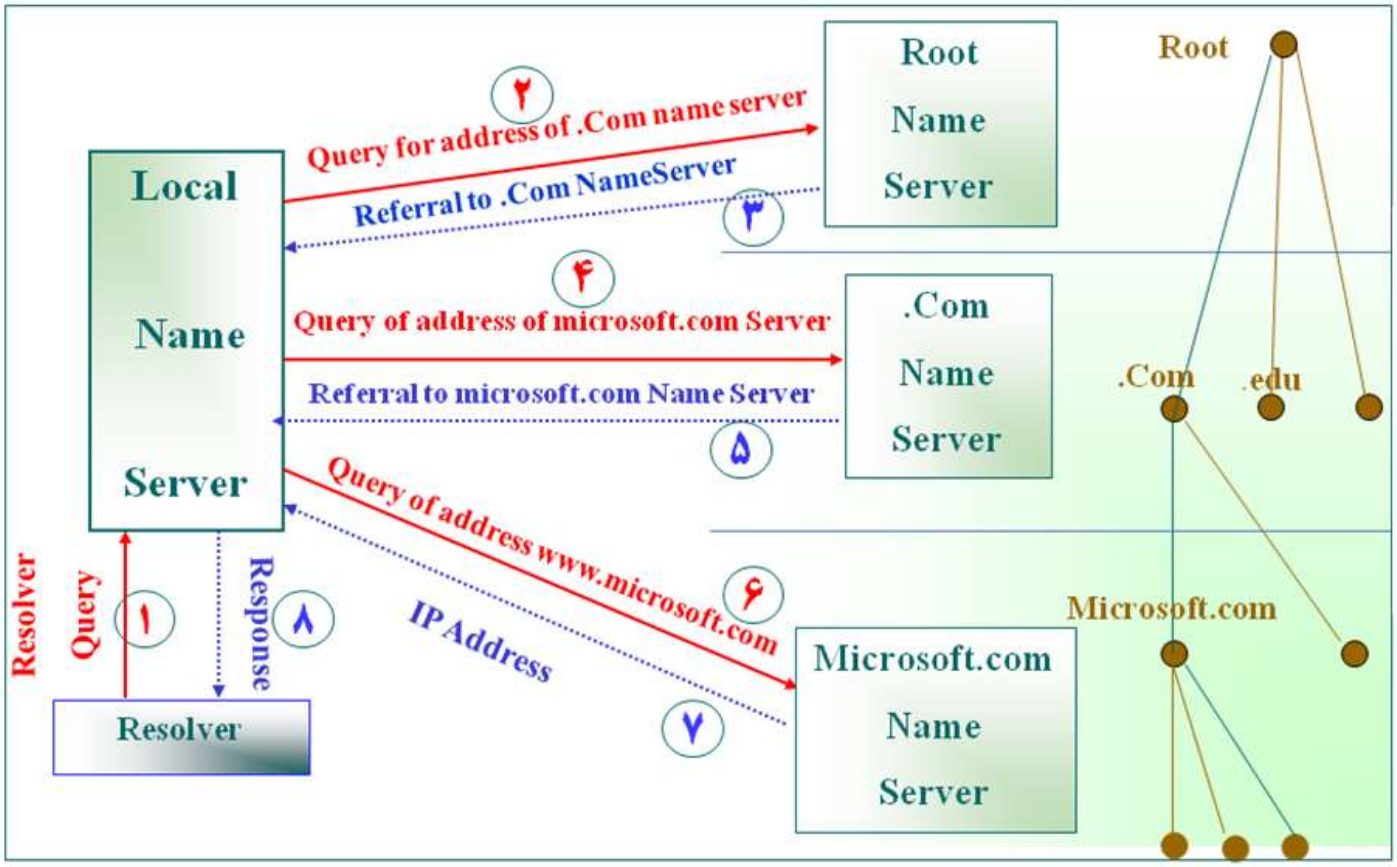
ولی اگر آن ناحیه در قلمرو سرویس دهنده های محلی نباشد، سرویس دهنده نام این درخواست را به سرویس دهنده نام سطح بالا ی ناحیه مزبور می فرستد.

۱۷-۷- انواع روش تبدیل Hostname به IP Address

یک سرویس گیرنده به منظور استفاده از DNS و اخذ پاسخ لازم از دو روش متفاوت استفاده می نماید. در مباحث زیر، منظور از کامپیوتر ISP، کامپیوتر های همان شرکتی است که کلاینت اینترنت خود را از آن می گیرد. مانند جهان گستر یا جهان روی خط.

۱۷-۷-۱- Non-Recursive Query (تکراری)

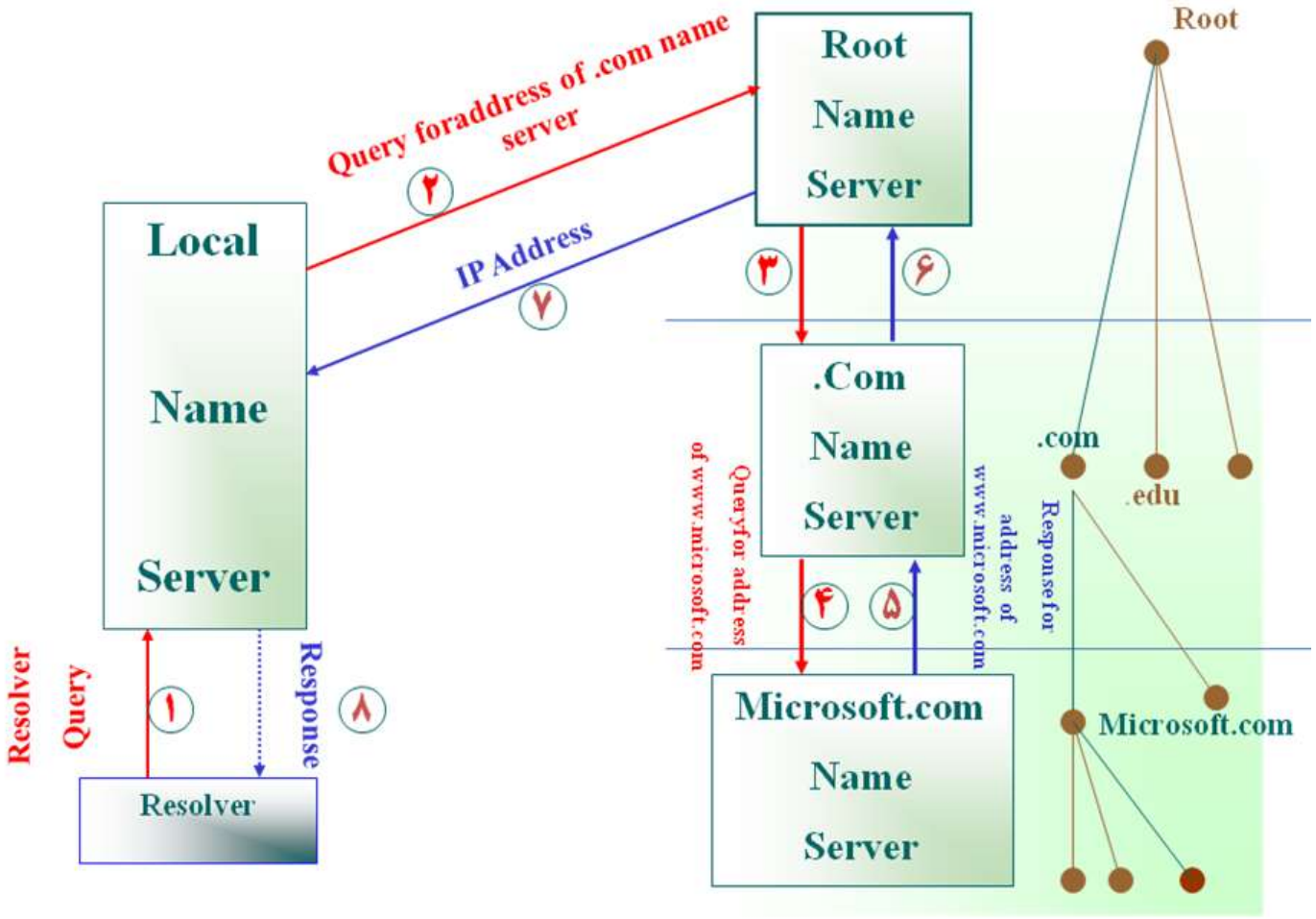
در این روش، کامپیوتر کلاینت، نام سرور مورد نظر را به سرور ISP خود می دهد و آدرس IP معادل آن را دریافت می کند. در این روش سرویس دهنده های موجود در ISP درگیر جزئیات می شوند. خود کامپیوتر های ISP با استفاده از DNS Server خود، از نگهدارنده های آدرس سطح بالاتر، آدرس کامپیوتر های سطح پایین تر را می پرسند و این کار را تا پیدا کردن آدرس نهایی تکرار می کنند. مثلاً برای آدرس www.Microsoft.com، ISP، از نگهدارنده .Com آدرس Microsoft.Com و سپس از Microsoft.Com، آدرس www.Microsoft.com را پرسیده و آدرس نهایی را به کاربر باز می گرداند. به عنوان مثالی دیگر، فرض کنید که قصد دارید آدرس Ramezani.ec.iut.ac.ir را به روش Non-Recursive Query (تکراری) استخراج کنید. بدین منظور، ابتدا کامپیوتر کلاینت درخواستی به کامپیوتر ISP داده و کامپیوتر DNS Server موجود در ISP نیز آدرس IP مربوط به DNS Server نگهدارنده آدرس های **ir.** را درخواست می کند (این سرور Hint Root است). پس از دریافت آدرس سرور نگهدارنده آدرس های .ir، مجددا کامپیوتر ISP درخواستی به سرور .ir داده و آدرس IP سرور ac.ir را تقاضا می کند. کامپیوتر ISP پس از یافتن آدرس IP مربوط به ac.ir، درخواستی به آن داده و آدرس iut.ac.ir را می طلبد. سپس آدرس ec.iut.ac.ir را از iut.ac.ir و آدرس Ramezani.ec.iut.ac.ir را از ec.iut.ac.ir تقاضا می کند. پس از پیدا شدن آدرس Ramezani.ec.iut.ac.ir، کامپیوتر ISP، آدرس نهایی را به کامپیوتر کلاینت می دهد.



ترجمه www.Microsoft.Com به روش تکراری

۱۷-۷-۲- Recursive Query (بازگشتی)

در این روش، نه کامپیوتر کلاینت و نه کامپیوتر ISP درگیر جزئیات یافتن آدرس IP نمی شوند. در این مثال، هر کامپیوتر DNS Serverی، آدرس کامپیوتر زیر مجموعه خود پیدا کرده و آن را بر می گرداند. مثلاً برای یافتن آدرس Ramezani.ec.iut.ac.ir، کامپیوتر کلاینت درخواست این آدرس را به ISP می دهد و ISP نیز این نام (Ramezani.ec.iut.ac.ir) را به نگهدارنده .ir می دهد. سپس نگهدارنده .ir نام را به نگهدارنده ac.ir می دهد. ac.ir نیز نام را به iut.ac.ir می دهد. iut.ac.ir نیز نام را به ec.iut.ac.ir می دهد و از آنجایی که ec.iut.ac.ir آدرس Ramezani را دارد (زیرا زیر مجموعه آن است)، آدرس آن را به iut.ac.ir می دهد. iut.ac.ir نیز آدرس را به ac.ir می دهد و ac.ir نیز آدرس را به نگهدارنده ir می دهد. در نهایت نیز ir آدرس را تحویل ISP داده و ISP نیز آدرس را به کلاینت می دهد. شکل زیر همین فرآیند را برای www.Microsoft.Com نشان می دهد.



ترجمه www.Microsoft.Com به روش بازگشتی

۱۷-۸- Cash Server

یکی دیگر از اجزای مورد استفاده در DNS، Cash Server می باشد که نقش زیادی در افزایش سرعت و کاهش ترافیک شبکه خواهد داشت. Cash Server پاسخ درخواست هایی را که قبلاً توسط DNS Client ها از آن پرسیده شده در حافظه خود نگه می دارد. به این ترتیب در صورتی که مجددا نیز به آن داشته باشد لازم به انجام مراحل Resolution نمی باشد و می تواند بلافاصله IP Address متناظر را برگرداند.

۱۷-۹- پروتکل DNS و مدل مرجع OSI

پروتکل DNS معمولاً از پروتکل UDP به منظور حمل داده استفاده می نماید. پروتکل UDP نسبت به TCP دارای سربار کمتری می باشد. هر اندازه سربار یک پروتکل کمتر باشد، سرعت آن بیشتر خواهد بود. در مواردی که حمل داده با استفاده از

پروتکل UDP با مشکل و یا بهتر بگوئیم خطا مواجه گردد، پروتکل DNS از پروتکل TCP به منظور حمل داده استفاده نموده تا این اطمینان ایجاد گردد که داده به درستی و بدون بروز خطا به مقصد خواهد رسید.

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

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

۱۷-۱۰- ساختار سرویس دهندگان نام دامنه ها در اینترنت

یک سرویس دهنده DNS، ضرورتی به آگاهی از تمامی اسامی دامنه های ثبت شده نداشته و صرفاً میزان آگاهی وی به یک سطح بالاتر و یک سطح پائین تر از خود محدود می گردد.

InterNic، مسئولیت کنترل دامنه های ریشه را برعهده داشته که شامل تمامی دامنه های های سطح بالا می باشد. در این بخش، تمامی سرویس دهندگان درDNS ریشه قرار داشته و آنها دارای آگاهی لازم در خصوص دامنه های موجود در سطح پائین تر از خود می باشند (مثلاًmicrosoft.Com). سرویس دهندگان DNS ریشه، مشخص خواهند کرد که کدام سرویس دهنده DNS در ارتباط با دامنه های.Com و یا .ir می باشد.

هر Domain شامل یک Primary DNS و یک Secondary DNS می باشد. Primary DNS، تمامی اطلاعات مرتبط با Domain خود را نگهداری می نماید. Secondary DNS به منزله یک Backup بوده و در مواردی که Primary DNS با مشکل مواجه می شود از آن استفاده می گردد (این سرور همان Alternate DNS Server می باشد که در مورد آن در بحث تنظیم آدرس IP در فصل دوم صحبت کردیم). به فرآیندی که بر اساس آن یک سرویس دهنده Primary DNS اطلاعات خود را در سرویس دهنده Secondary DNS تکثیر می نماید، **Zone Transfer** گفته می شود. با توجه به این که هم اینک میلیون ها وب سایت وجود دارد و هر روز نیز به تعداد آنها اضافه می گردد، عملاً روشی وجود ندارد که بتوان با یک سرویس دهنده DNS، تمامی آدرس های IP را در آن ذخیره و این سرویس دهنده نیز قادر باشد به هر درخواستی جهت اتصال به اینترنت پاسخگو باشد. علاوه بر این، ایده استفاده از یک سرویس دهنده متمرکز می تواند هدف خوبی برای مهاجمان به منظور از کار انداختن آن باشد.

در مقابل استفاده از یک سرویس دهنده DNS متمرکز، سرویس دهندگان DNS توزیع شده اند. بنابراین یک سرویس دهنده DNS دارای تمامی اسامی Host ها و آدرس های IP برای تمامی شبکه اینترنت نخواهد بود. سازمان ICANN (برگرفته از Internet Corporation for Assigned Names and Numbers)، مسئولیت ثبت تمامی اسامی دامنه ها بر روی اینترنت را برعهده دارد.

مثال:

برای آشنائی با فرآیند یافتن نام یک وب سایت، فرض کنید قصد مشاهده وب سایت http://www.Google.Com را داشته باشیم. پس از تایپ آدرس فوق، مرور گر آدرس درخواستی را برای سرویس دهنده DNS که توسط پیکربندی TCP/IP بر روی کامپیوتر شما مشخص شده است ارسال می نماید (هنگام اتصال به اینترنت، بر اساس تنظیمات شرکت سرویس دهنده اینترنت یا ISP، آدرس DNS Server شما نیز تغییر خواهد نمود). فرض کنید سرویس دهنده DNS شما نسبت به آدرس IP

وب سایت فوق آگاهی نداشته باشد. بنابراین آن را برای سرویس دهنده DNS مربوط به ICANN ارسال می نماید. DNS فوق آدرس IP وب سایت فوق را نمی داند، ولی از آدرس IP سرویس دهنده DNS مرتبط با نام دامنه ای که به Com. ختم می شود آگاهی دارد. در ادامه، آدرس سرویس دهنده DNS مربوط به دامنه درخواستی (در این مثال Google.Com) برای مرور گر شما ارسال خواهد شد و در نهایت درخواستی برای سرویس دهنده DNS مربوط به دامنه ارسال تا آدرس IP کامپیوتری با نام www مشخص و برای متقاضی بازدید از وب سایت برگردانده شود.

۱۷-۱۱- DNS و WINS (Windows Internet Naming Service)

۱۷-۱۱-۱- DNS

سرویس DNS، توسط کامپیوتر هایی که بر روی آنان یک سرویس دهنده DNS اجراء شده است، ارائه می گردد. سیستم های عامل ویندوز تقریباً با هر نوع سرویس دهنده DNS استاندارد سازگار می باشند. (مثلاً سرویس دهندگانی که بر روی سیستم عامل یونیکس اجراء می گردند). ویندوز دارای نسخه اختصاصی خود در رابطه با سرویس دهنده DNS بوده که می توان آن را بر روی هر نوع سیستم عامل ویندوز (۲۰۰۳ و یا دات نت)، نصب نمود.

۱۷-۱۱-۲- تفاوت بین DNS و WINS چیست؟

WINS، به منظور ترجمه اسامی کامپیوتر ها به آدرس های IP، استفاده می گردد (دقیقا مانند DNS، اما WINS قدیمی تر بوده و با برخی سیستم ها سازگاری ندارد). اسامی استفاده شده در WINS، نوع خاصی از نام های مبتنی بر ویندوز های قدیمی (x۹ و Me) می باشند. DNS، به مراتب متداول تر بوده و از آن به منظور ترجمه اسامی میزبان استفاده می شود. در محیط ویندوز، تفاوت زیادی بین دو نوع نام (اسامی خاص مبتنی بر ویندوز و اسامی میزبان) وجود نداشته و هر دو نوع، معادل می باشند. از نسخه ویندوز ۲۰۰۰ به بعد، تاکید مضاعف بر استفاده از DNS در دستور کار قرار گرفته و مایکروسافت، استفاده محدود و کم رنگ WINS را به عنوان یک سیاست محوری در ویندوز دنبال می نماید.

به منظور پیکربندی IP هریک از کامپیوتر های موجود در شبکه، می بایست آدرس IP و حداقل یک سرویس دهنده DNS را مشخص کرد. در این رابطه نمی توان از نام سرویس دهنده DNS در مقابل آدرس IP، استفاده نمود. (روشی به منظور ترجمه اسامی به آدرس IP بدون یک سرویس دهنده DNS وجود ندارد).

DDNS (DNS پویا)، امکان به هنگام سازی پویای سرویس دهنده DNS را برای کامپیوتر ها فراهم می نماید. بدین ترتیب، بانک اطلاعاتی DNS شامل آخرین اطلاعات مرتبط با آدرس هایIP موجود در شبکه، شده و سرویس دهنده DNS، قادر به ارائه سرویس خود به صورت پویا و متاثر از آخرین تغییرات انجام شده در شبکه، خواهد بود.

به منظور کاهش حجم عملیات مربوط به Name Resolution در یک محیط عملیاتی بزرگ، می توان از یک سرویس دهنده ثانویه و یا سرویس دهندگان Caching، استفاده کرد (که قبل تر توضیح داده شد). سرویس دهنده ثانویه، دارای بانک اطلاعاتی اختصاصی خود نبوده و از بانک اطلاعاتی DNS موجود بر روی یک سرویس دهنده DNS اولیه، استفاده می نماید. سرویس دهندگان ثانویه، گزینه ای مناسب برای ارائه خدمات مربوط به Name Resolution بوده ولی قادر به بهنگام سازی پویای DNS نخواهند بود. (برخی از انواع سرویس دهندگان ثانویه قادر به دریافت اطلاعات بهنگام شده و ارسال آنان برای سرویس دهنده اولیه، می باشند). سرویس دهندگان Caching DNS، زمانیکه یک درخواست Name Resolution را دریافت می نمایند، با یک سرویس دهنده DNS به منظور اتمام عملیات خود، ارتباط برقرار خواهد کرد. سرویس دهنده Caching، در ادامه آدرس IP را استفاده و آن را به منظور پاسخ به درخواستی مشابه، ذخیره می نماید.

۱۷-۱۲- نصب DNS در ویندوز سرور ۲۰۰۳

نرم افزار سرویس دهنده DNS ویندوز، امکان ذخیره داده های DNS را در یک فایل متن و یا در اکتیو دایرکتوری، فراهم می نماید. با انتخاب اکتیو دایرکتوری، دارای گزینه ای مبنی بر نصب DNS بر روی هر Domain Controller خواهیم بود. در

چنین مواردی در صورت بروز اشکال در اکتیو دایرکتوری، امکان بازیابی سریع اطلاعات وجود خواهد داشت (می توان DNS را بر روی یک Domain Controller دیگر نصب تا زمینه استفاده از اطلاعات DNS موجود در اکتیو دایرکتوری، فراهم گردد).

۱۷-۱۲-۱- تنظیم آدرس IP

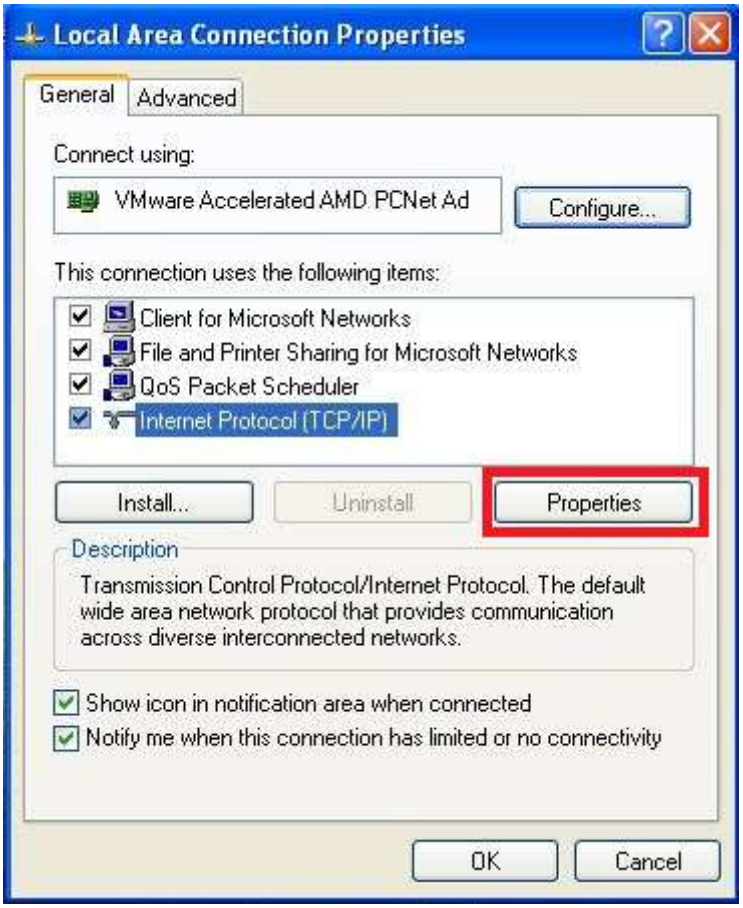
قبل از نصب DNS، بایستی تنظیمات TCP/IP را انجام دهیم. اولین کار تنظیم آدرس IP به صورت Static است. البته این کار را می توان بعدا نیز انجام داد.

برای انجام تنظیمات IP، وارد مسیر زیر شوید:

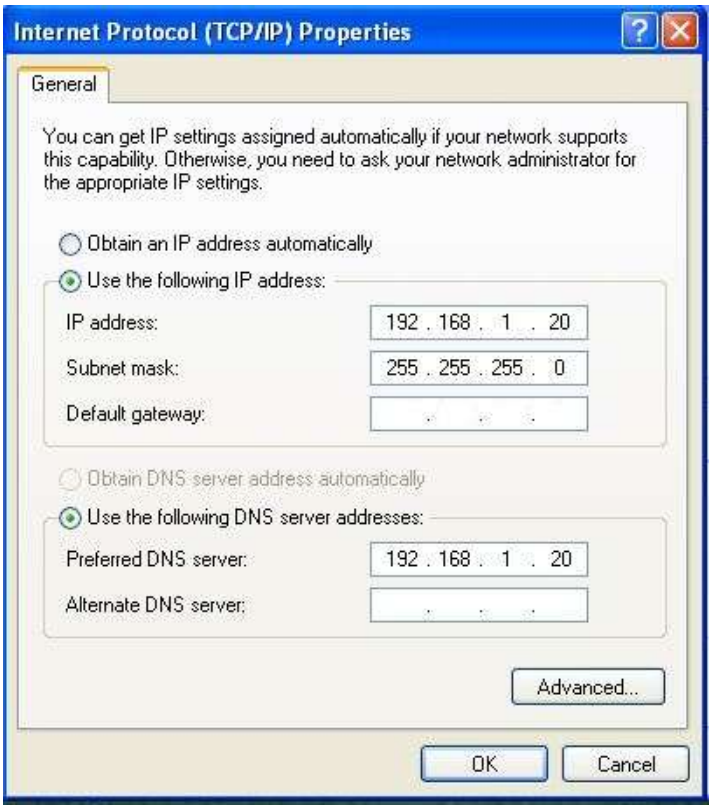
Control Panel ➔ Network Connections

روی Local Area Network راست کلیک کرده و Properties را انتخاب نمایید.

در صفحه باز شده، گزینه Internet Protocol (TCP/IP) را انتخاب کرده و سپس روی دکمه Properties کلیک نمایید.



در صفحه باز شده، مانند شکل، آدرس IP را به صورت دستی تنظیم کنید. در قسمت Preferred DNS نیز آدرس DNS Server که نصب کرده اید را وارد نمایید.

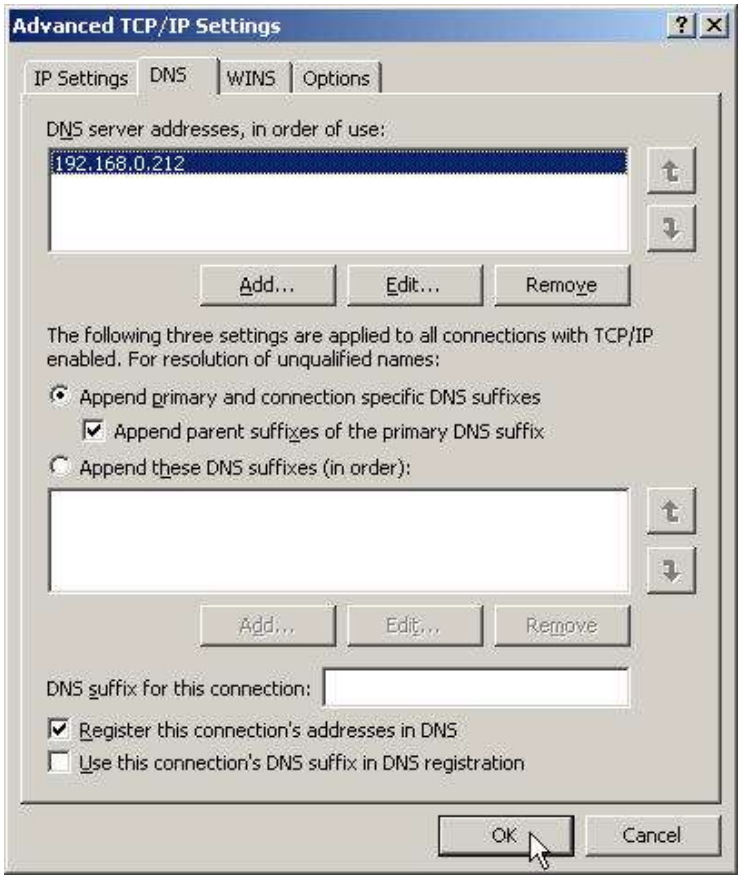


سپس روی دکمه Advanced کلیک کرده و سربرگ DNS را انتخاب کنید. سپس ۳ کار زیر را انجام دهید:

۱- گزینه Append primary and connection specific DNS suffixes را انتخاب کنید.

۲- خانه Append parent suffix of the primary DNS suffix را چک مارک کنید.

۳- خانه Register this connection's address in DNS را نیز چک مارک کنید.



سپس OK کنید تا پنجره بسته شود. حال نوبت به نصب DNS می شود.

۱۷-۱۲-۲- نصب DNS از طریق آدرس دهی

برای انجام کار به صورت زیر عمل کنید:

Start → Setting → Control Panel → Add/Remove Program →Add/Remove Components →Select Networking Service (do not tick) →Details → Tick DNS (Domain name system) →Ok →Next → Finish

۱۷-۱۲-۳- نصب DNS از طریق شکل

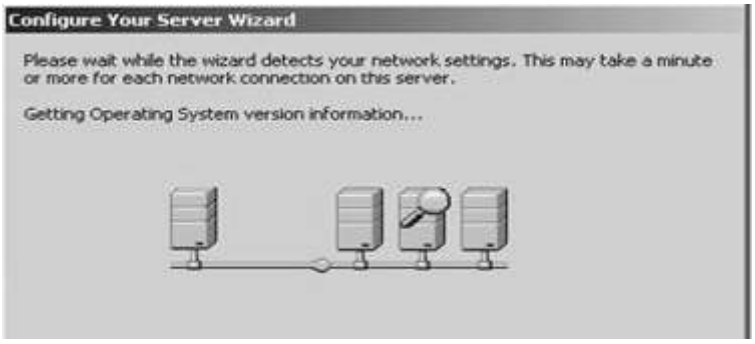
برای انجام کار به صورت زیر عمل کنید:

Start → Administrative Tools → Configure Your Server Wizard

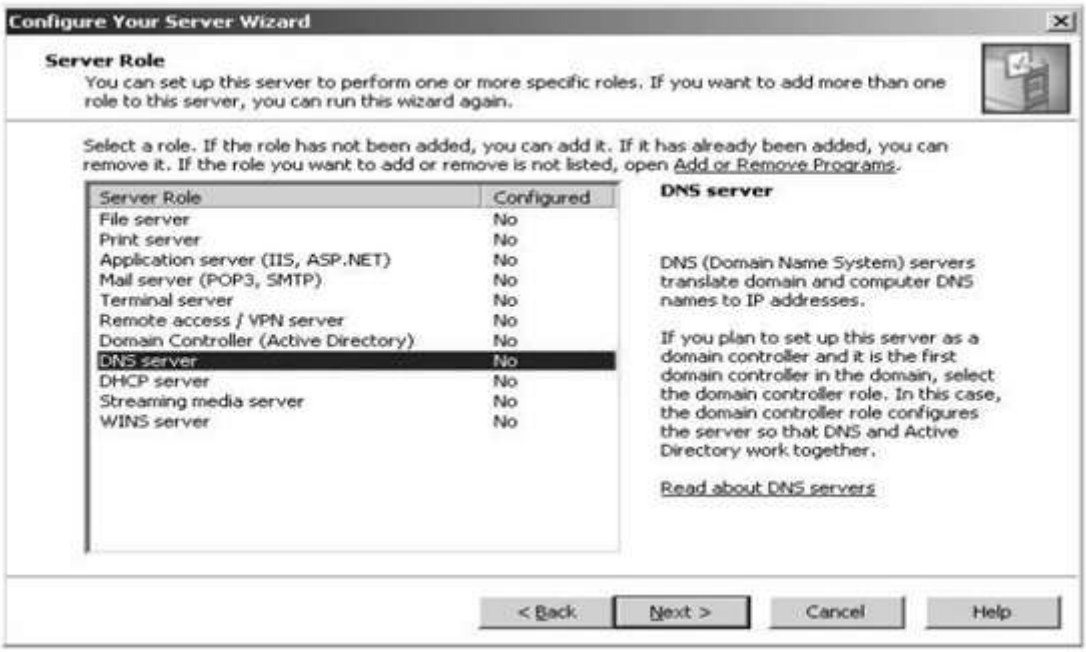
صفحه خوش آمدگویی باز می شود. در این صفحه Next بزنید تا به صفحه بعد بروید.

مجددا Next بزنید تا به صفحه بعد بروید.

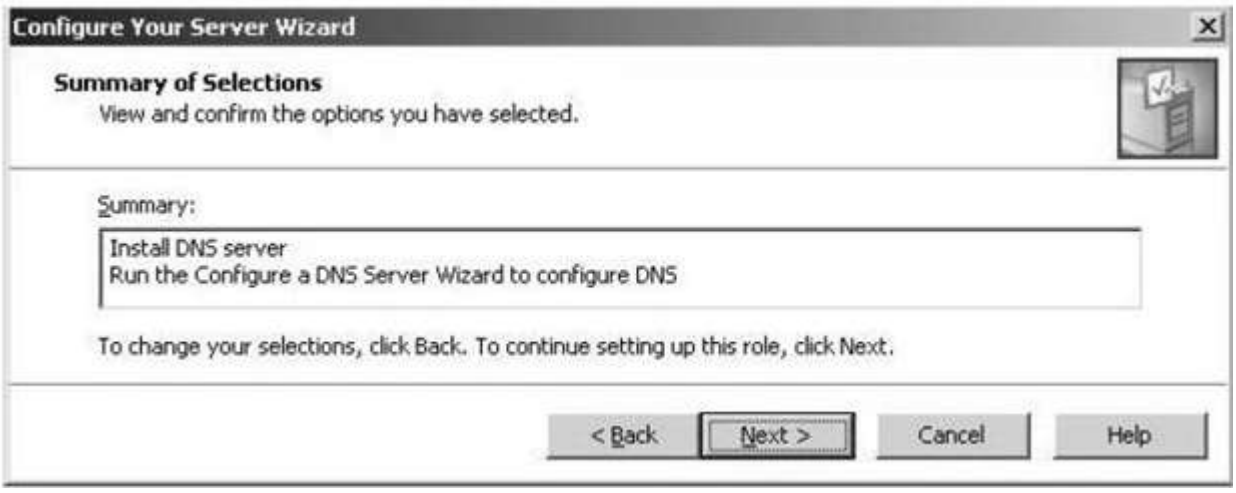
صبر نمایید تا این صفحه بسته شود.



در صفحه باز شده، گزینه DNS را انتخاب نمایید؛ تا سرور شما نقش DNS Server را بپذیرد.



مجددا Next بزنید تا به صفحه بعد بروید.



مدتی صبر نمایید تا سیستم، DNS Server را نصب نماید.

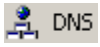
در نهایت روی دکمه Finish کلیک کنید تا عملیات نصب، پایان پذیرد.

بعد از انجام عملیات نصب DNS آن را اجرا میکنیم تا از کارکرد درست کابل شبکه اطمینان به عمل آوریم.

۱۷-۱۳- پیکربندی DNS Server

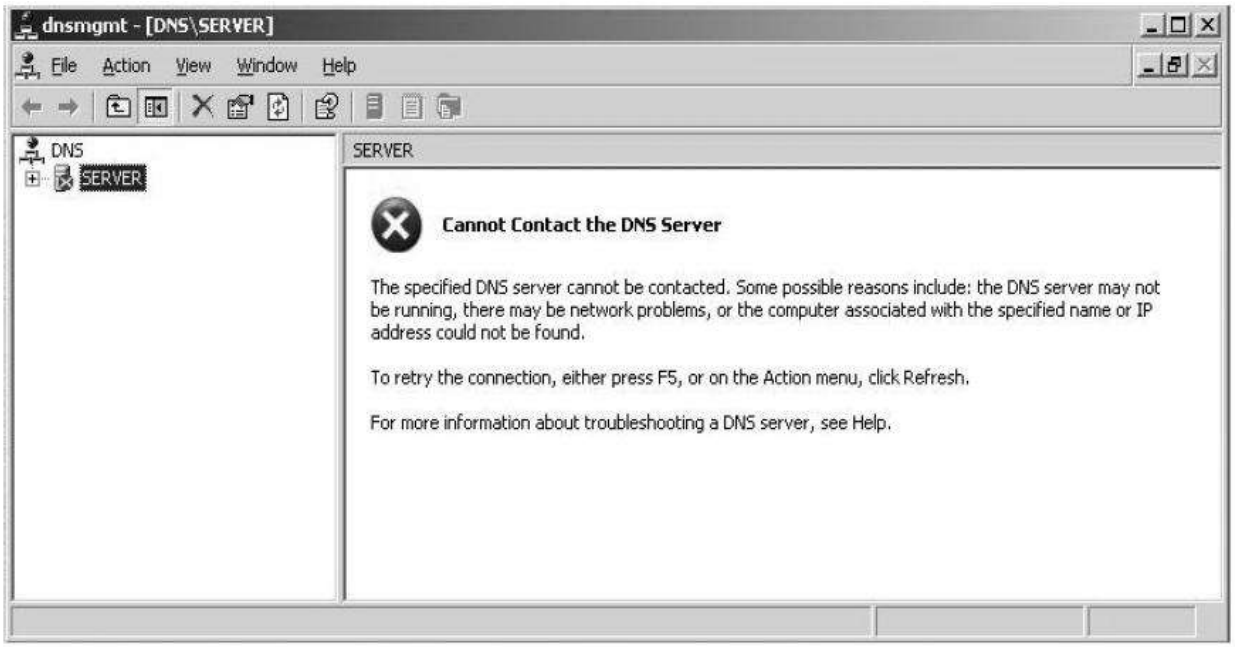
برای پیکربندی DNS Server، مراحل زیر را دنبال نمایید:

Start→Administrative Tools→ DNS



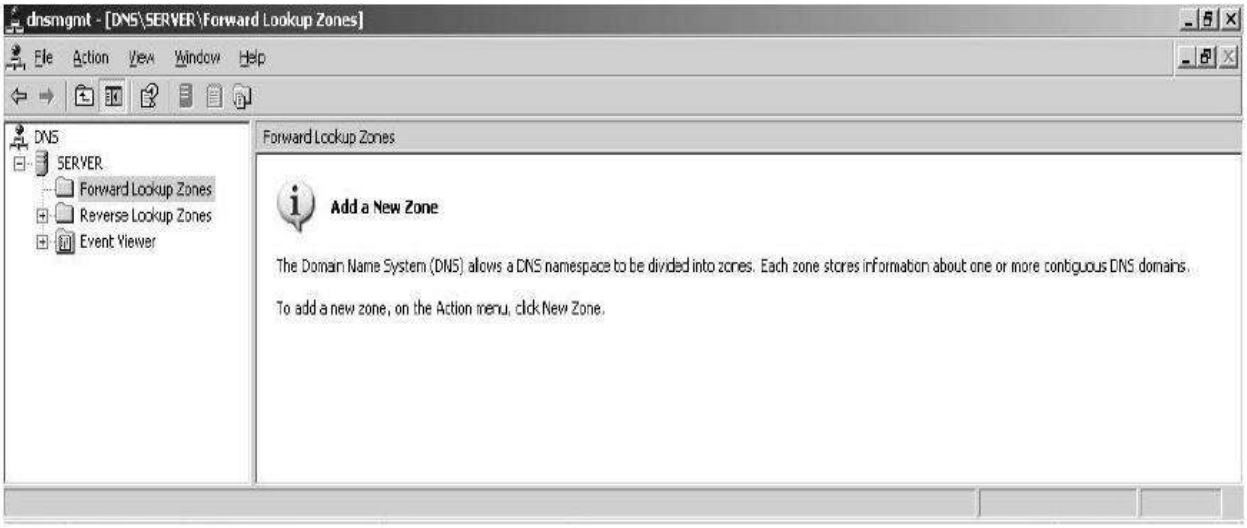
بعد از اجرای DNS دو حالت وجود دارد که به صورت زیر می باشند:

اگر شکل DNS – [with problem] را مشاهده کردید در اینصورت از صحت عملکرد کابل شبکه خود اطمینان حاصل فرمایید و یا اینکه کابل شبکه را جدا کرده و آن را مجددا وصل کنید.



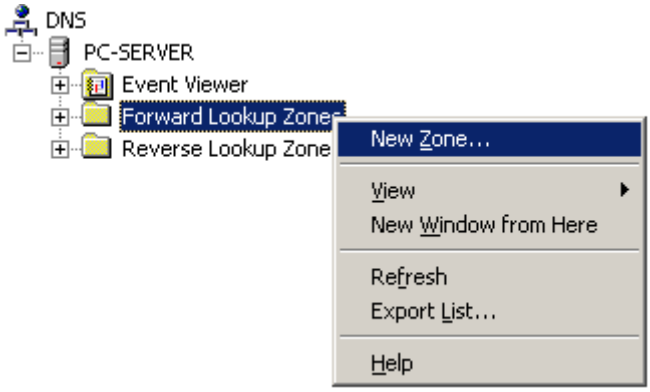
شکل DNS – [with problem]

اگر شکل DNS – [no problem] را مشاهده کردید، در اینصورت در ادامه بحث، همراه ما باشید.

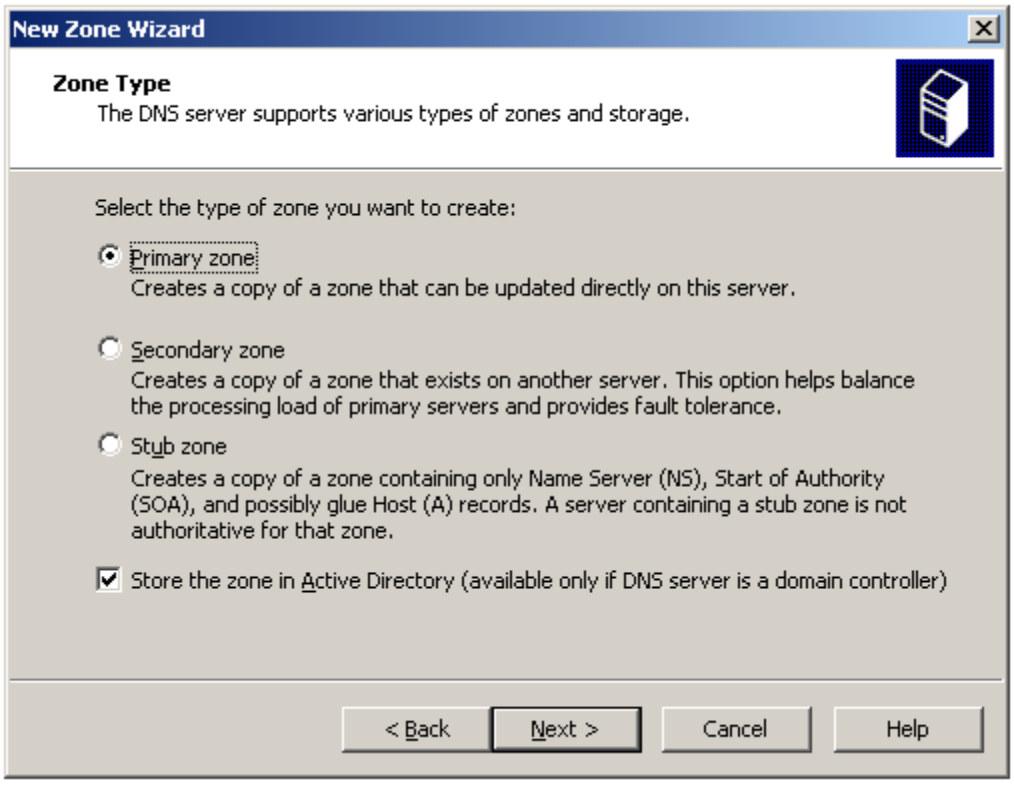


شکل DNS – [no problem]

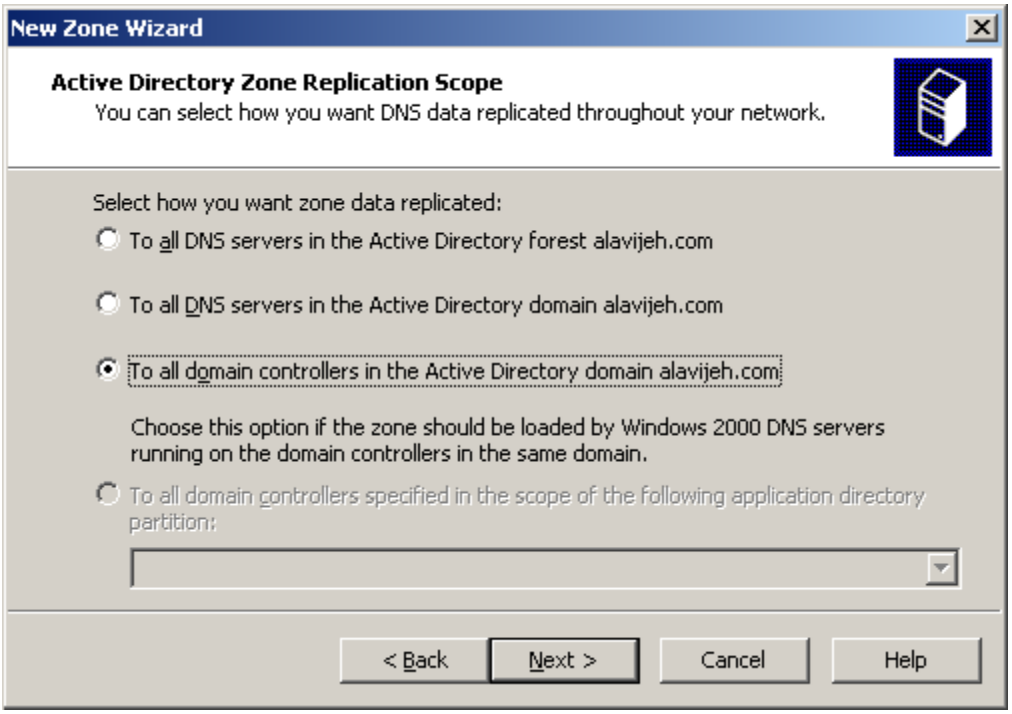
پس از اجرای صحیح، پنجره ای ظاهر می شود که در قسمت درختی آن نام سرویس دهنده و در زیر آن دو عبارت Forward Lookup Zones (تبدیل Hostname بـه IP Address) و Reverse Lookup Zones (تبـدیل IP Address بـه Host Name) نمایش داده می شود. برروی Forward راست کلیک کرده و گزینه New Zone را انتخاب کنید (Zone محلی برای نگهـداری اطلاعات اسامی یک یا چند دامنه یا زیر دامنه است).



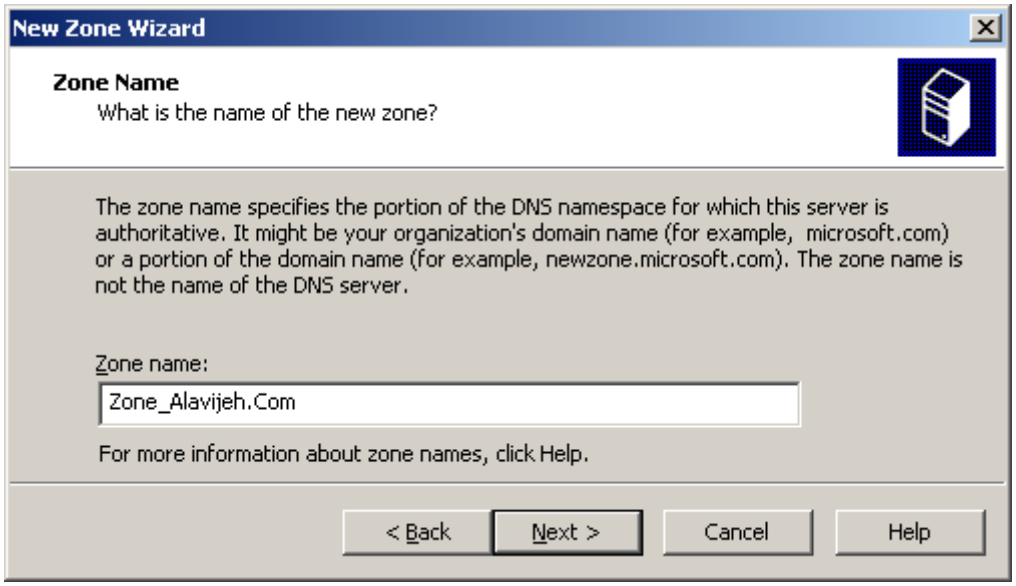
بعد از انجام این کار باید نوع ناحیه را مشخص کنیم، پیش فرض (Standard) را قبول کرده و دکمه Next را بزنید. گزینه Standard Secondary مربوط به Backup DNS و گزینه Stub zone، شامل بخشی از Primary Zone می باشد. اگر این اولین Zoneی است که دارید ایجاد می کنید، فقط قابلیت انتخاب گزینه Primary zone را دارید.



اگر Active Directory را نصب کرده باشید، صفحه زیر را مشاهده خواهید نمود. گزینه آخر را انتخاب کرده و Next بزنید. این صفحه بیان می کند که شما قصد دارید این Zone با کدام قسمت ها عمل Replicate را انجام دهد؟



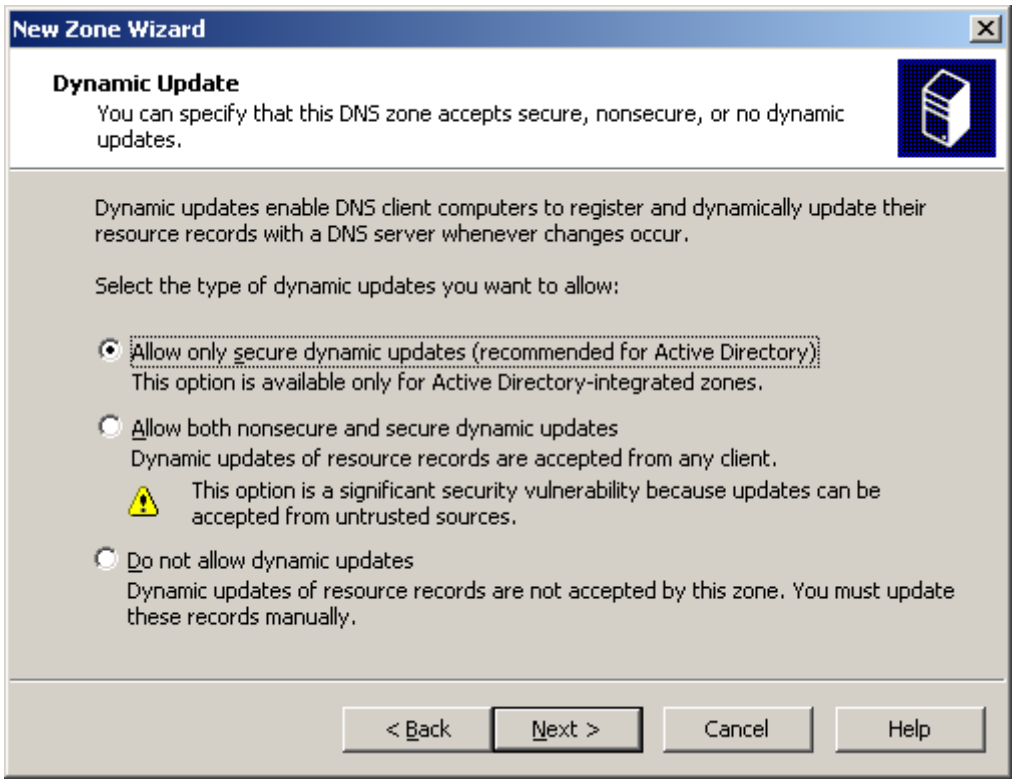
در پنجره بعدی نام Zone خود را وارد کنید، مثلاً Zone_Alavijeh.Com. البته توصیه می شود که نام Zone با نام دامنه ای که دارید برابر باشد یا بسیار به آن شبیه باشد تا یک دسته بندی منطقی از Zoneها داشته باشید.



در پنجره بعدی، فایل DNS ساخته می شود. نام فایل را وارد کرده و Next را بزنید.

:Dynamic Update

به فرآیندی گفته می شود که براساس آن Client ها اطلاعات خود را به صورت اتوماتیک درون DNS ثبت می کنند. در پنجره بعدی مشخص نمایید که به روز رسانی اطلاعات DNS به چه صورت باشد؟ اگر Active Directory نصب شده باشد، توصیه می شود که به روز رسانی امن را انتخاب کنید (گزینه ۱). گزینه دوم عملیات به روز رسانی را هم به صورت امن و هم به صورت نا امن (از منابع تایید نشده) انجام می دهد. گزینه سوم نیز به روز رسانی را انجام نمی دهد. در نهایت روی Next کلیک کنید.



:Forwarder

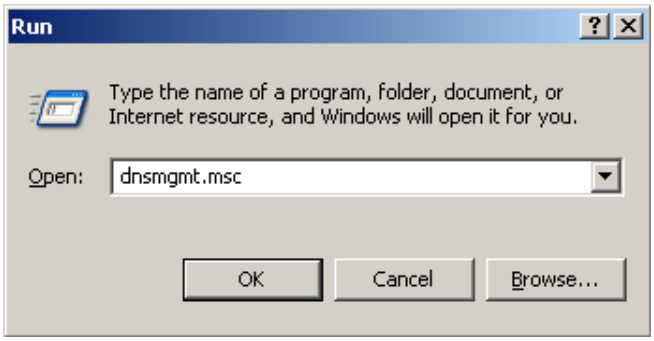
در صورتی که DNS Server موفق به پاسخگویی به Client ها نشود، می تواند آن را به یک DNS دیگر که Forwarder نام دارد، بفرستد. در صورتیکه نمی خواهید اطلاعات را Forward کنید گزینه دوم یعنی No, it should not forward queries را انتخاب کنید. با انتخاب این گزینه DNS Server جهت عملیات Resolution به Root Server ها مراجعه می کند.

برای ادامه کار دکمه Next را بزنید.

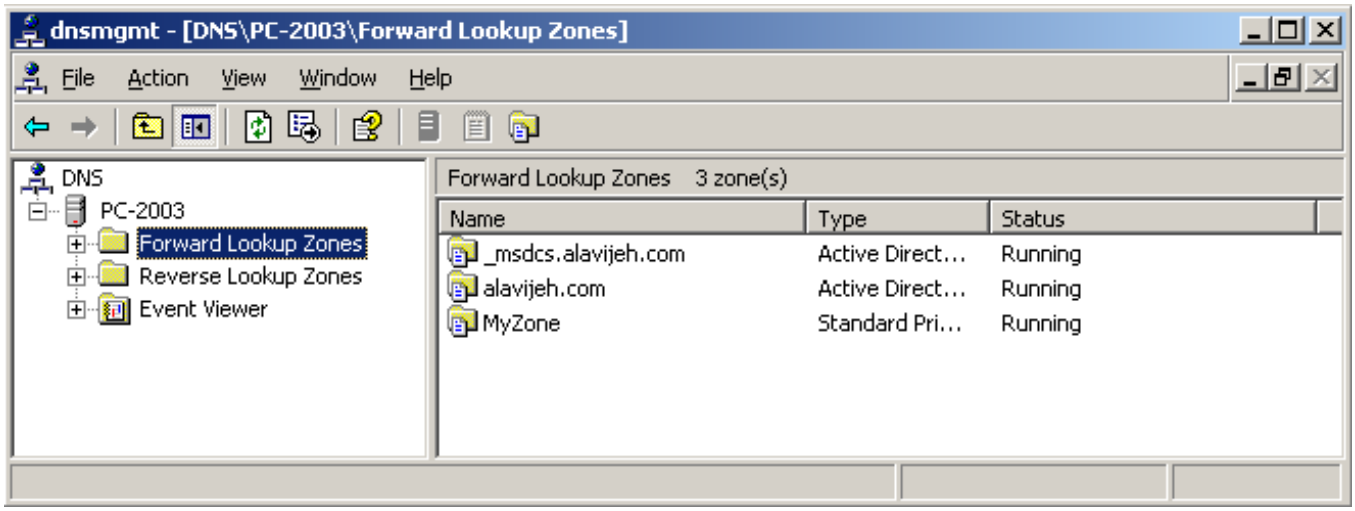
با زدن دکمه Next، DNS Server به دنبال Root Hint های تعریف شده که در واقع آدرس سرورهای Root میباشد، خواهد گشت. در نهایت دکمه Finish را کلیک کنید تا مراحل تکمیل گردد.

۱۷-۱۴- تنظیمات DNS Server

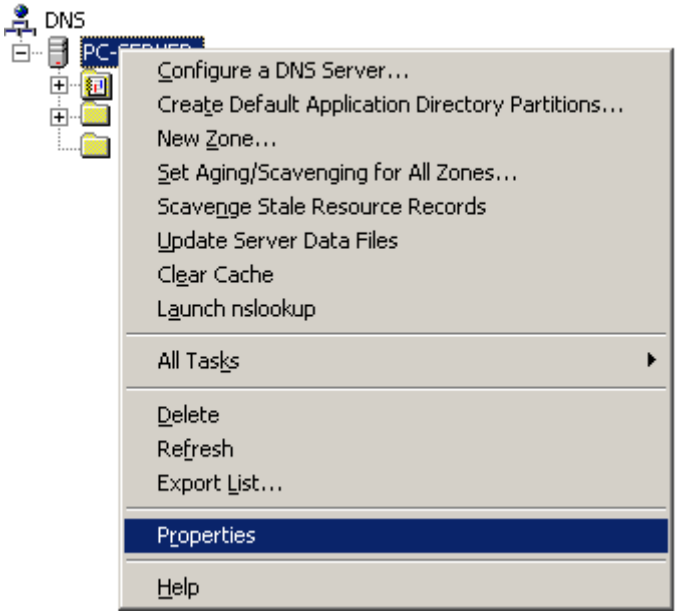
در درون گزینه RUN تایپ کنید: dnsmgmt.Msc، یا از طریق Start➔Administrative Tools➔DNS، صفحه کاربری DNS را باز نمایید.



در پنجره باز شده در سمت چپ یک ساختار درختی شامل نام DNS Server و زیر مجموعه های آن یعنی Forward lookup zones، Reverse lookup zones و Event viewer قرار دارد.



بر روی نام سرور راست کلیک کنید و گزینه Properties را انتخاب کنید.



پنجره ای شامل چند Tab برای تنظیمات DNS Server باز می شود.

از طریق این Tabها می توانید تنظیمات مربوط به DNS Server را انجام دهید. توجه نمایید که برخی از این سربرگ ها بسیار تخصصی بوده و در موارد و شرایط خاصی استفاده می شوند؛ لذا ما نیز آن ها را با جزئیات مورد بررسی قرار نمی دهیم.

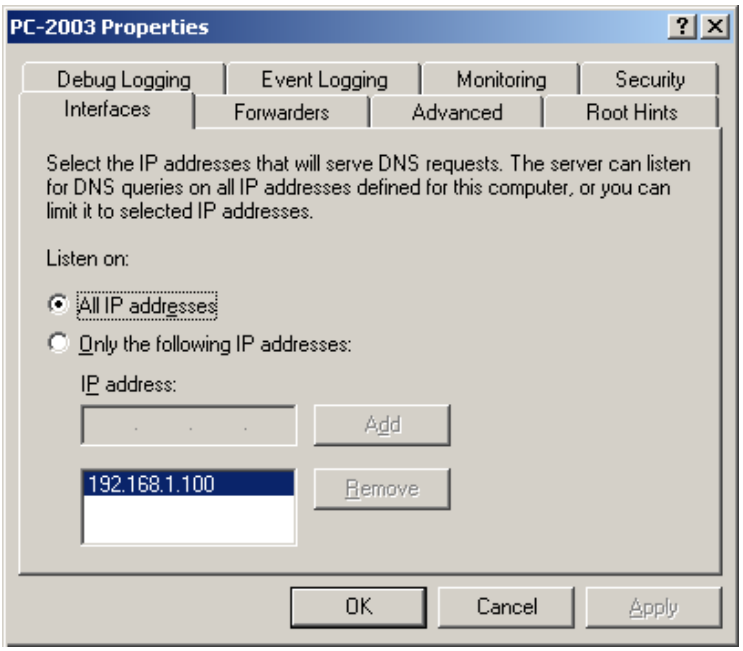
نکته حائز اهمیت این می باشد که کار کردن با تنظیمات DNS Server در صورتی مفید خواهد بود که کاربر مفاهیم پایه و اولیه DNS Server، آدرس های IP، Address Resolution، سلسله مراتب آدرس دهی و آدرس یابی، پروتکل های TCP و UDP، فرآیند امنیت و سطوح دسترسی را به خوبی درک کرده و با آن ها آشنا باشد.

لذا توصیه اکید بنده، قبل از ورود به تنظیمات DNS Server این می باشد که ابتدا حتما با مفاهیم فوق آشنا شده و سپس وارد قسمت تنظیمات DNS Server شوید.

در ادامه، به معرفی سربرگ های تنظیمات DNS Server خواهیم پرداخت.

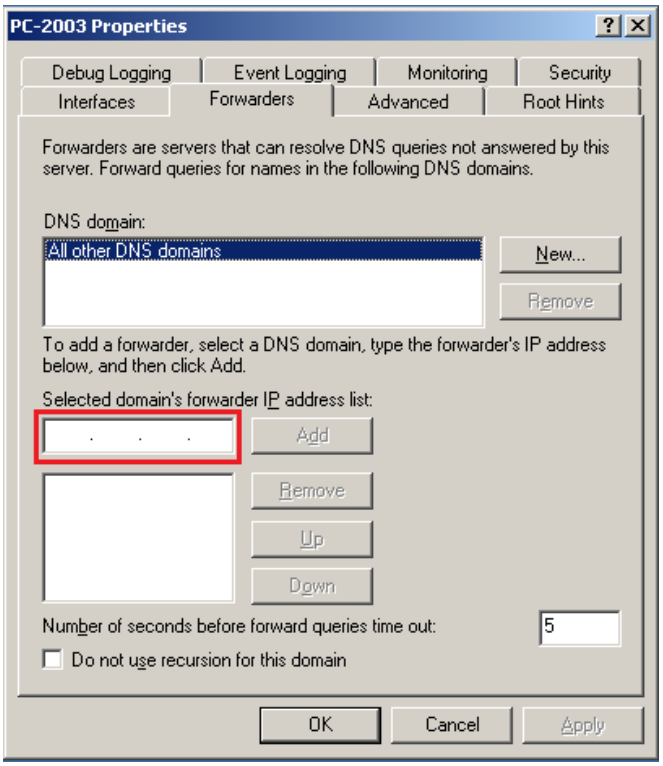
۱- Interfaces

این سربرگ نشان دهنده آدرس IP کارت شبکه ای است که این سرور از طریق آن درخواست های Client ها را دریافت می کند.



۲- Forwards

مشخص کننده آدرس DNS server هایی می باشد که در صورتی که این سرور موفق به Resolve، name به IP نشود از آنها به منظور عملیات Resolution کمک می گیرد.

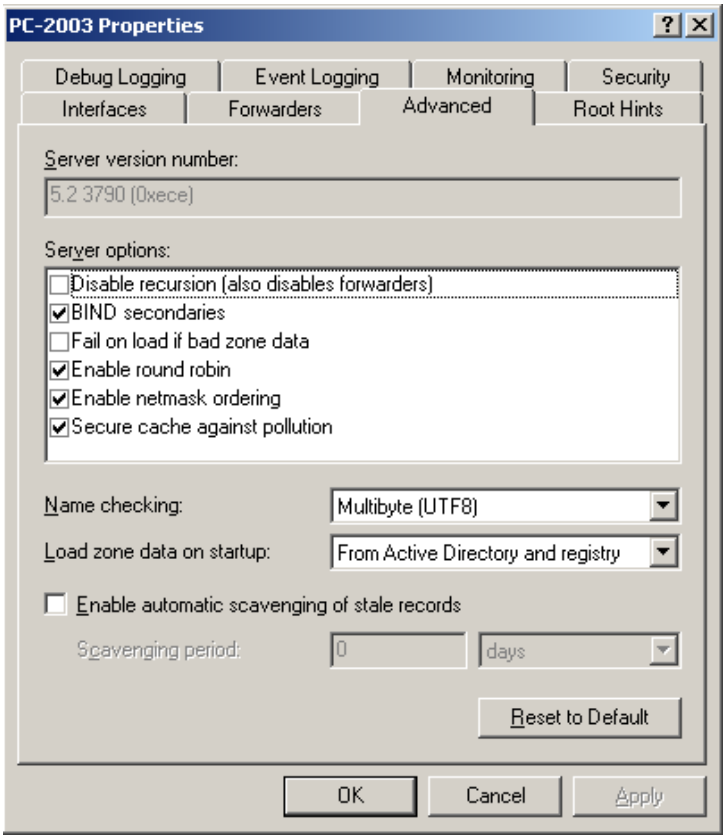


فعال سازی DNs Forwarding برای اتصالات اینترنت

برای این کار، در همین صفحه، در جای مخصوص آدرس IP، آدرس IPمربوط به سرور DNS که قرار است بـه عنـوان ISP مـا باشد را وارد کرده و OK را می زنیم (قسمت قرمز رنگ تصویر بالا).

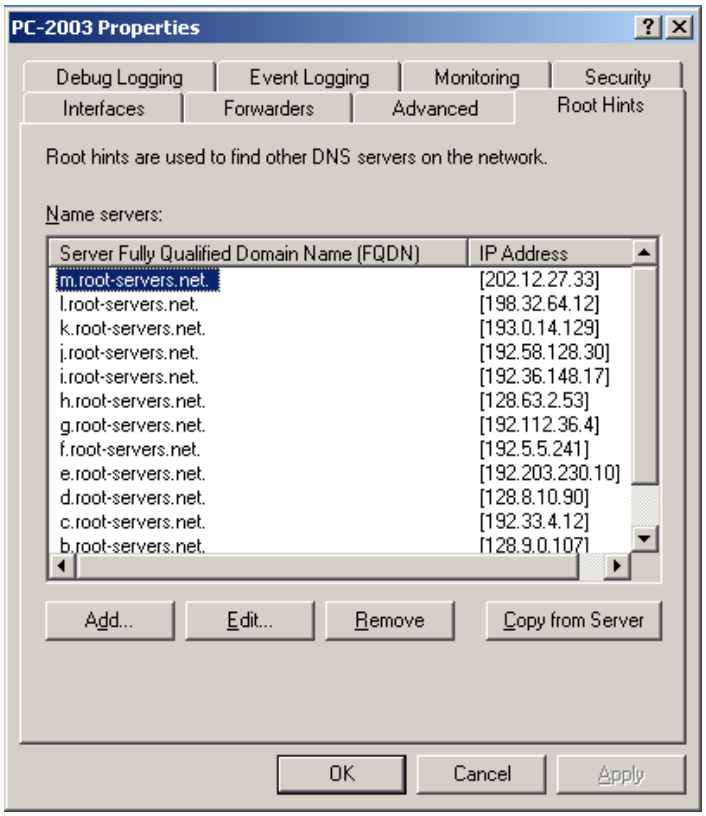
۳- Advanced

حاوی option های خاصی در مورد سرور می باشد. مثل تنظیمات امنیتی و کنترل بار (Load) زیاد.



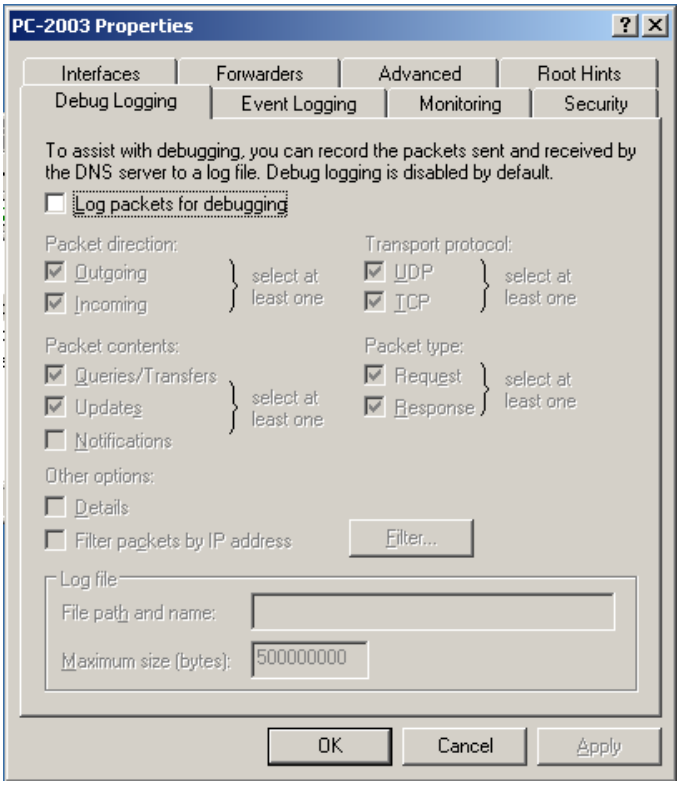
۴- Root hints

آدرس سرورهای Root می باشد که به صورت پیش فرض در آن گنجانده شده است ولی می توانید آدرس جدیدی نیز بـه آن اضافه کنید.



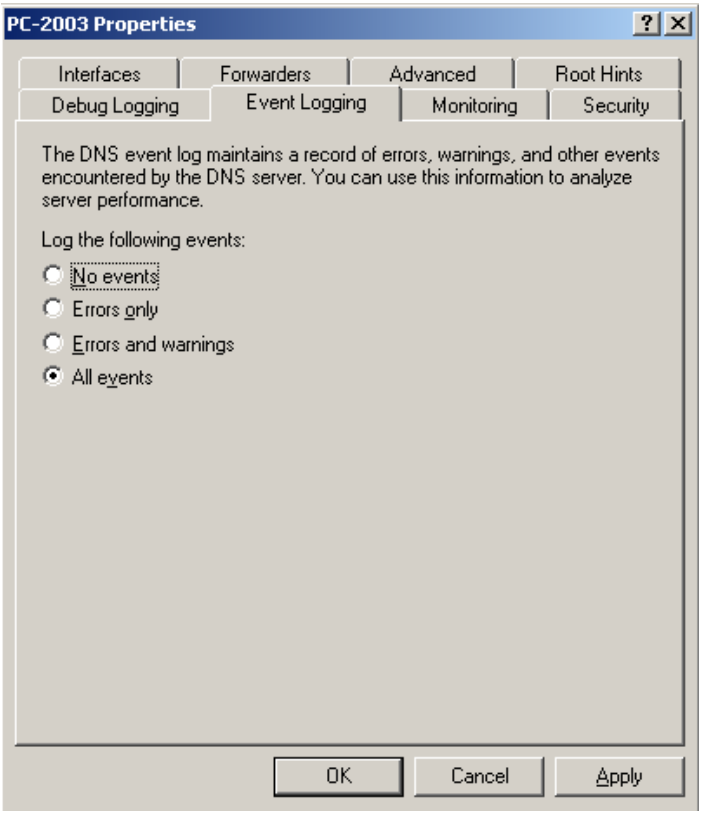
۵- Debug logging

در این سربرگ می توانید نوع Packet هایی که می خواهید اطلاعات آن ها ذخیره شود، مشخص کنیـد. ایـن اطلاعـات درون یک Log file ذخیره می شود و به طور پیش فرض این ابزار غیر فعال می باشد.



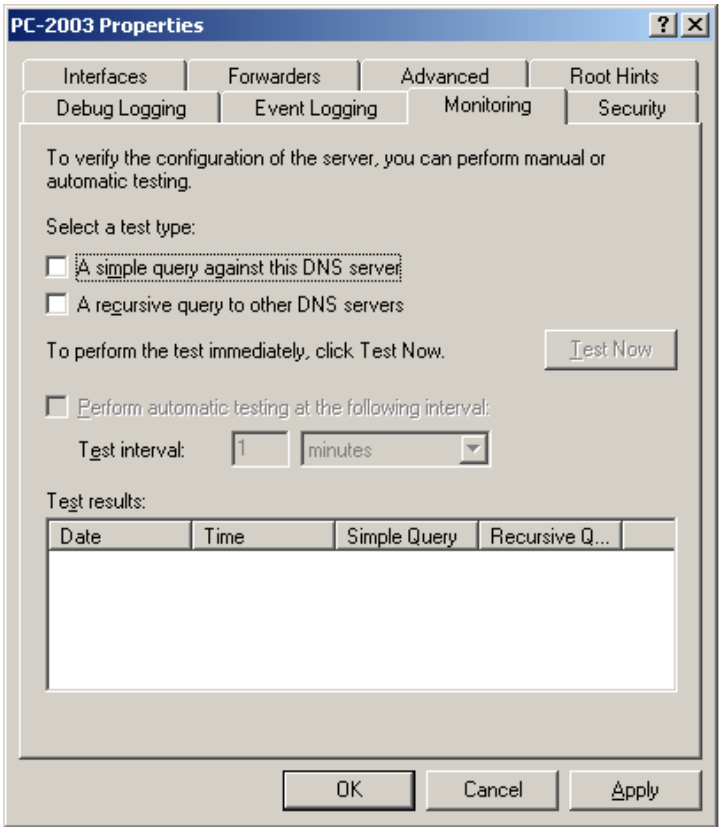
۶- Event logging

در این سربرگ، نوع Event هایی را که می خواهید درون Event viewer ذخیره گردند را مشخص کنید.



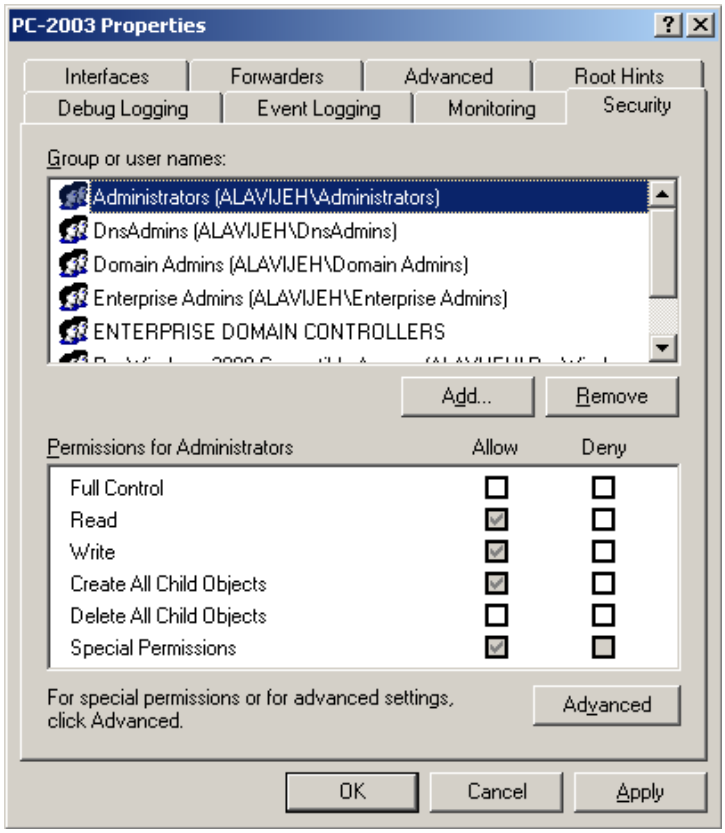
۷- Monitoring

این سربرگ، امکاناتی در جهت تست صحت کارکرد DNS را برای شما فراهم میکند.



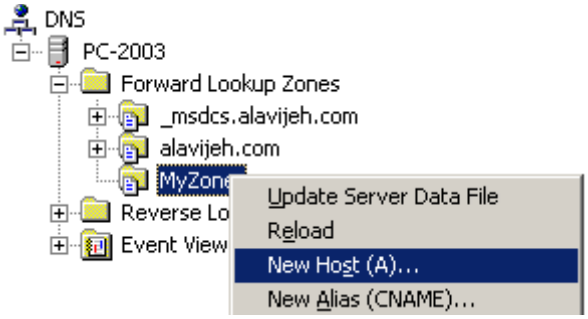
۸- Security

مشخص کننده گروه ها و اعضای آنها، از جمله DNS Admin که توانایی ایجاد و اعمال تغییرات در DNS را دارا است، می باشد.

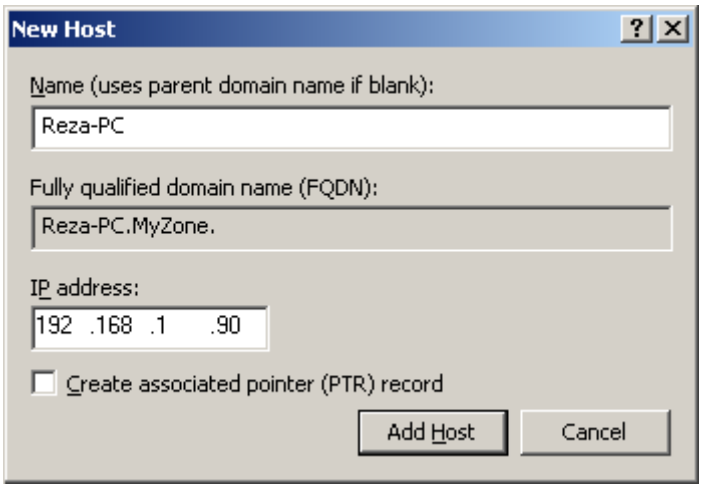


۱۷-۱۵- ایجاد Host جدید

اکنون وقت آن می رسد که رکورد جدیدی را تعریف کرده و اطلاعات یک کامپیوتر + آدرس IP آن را وارد نمایید. بدین منظور روی Zone ساخته شده، راست کلیک کرده و گزینه New Host را انتخاب کنید. مطابق شکل، قابلیت تعریف انواع رکورد وجود دارد. انواع رکورد را در ابتدای این فصل معرفی کرده ایم. در اینجا قصد داریم رکوردی از نوع A (Hostname ➔ IP Address) بسازیم.



سپس در صفحه باز شده، ابتدا نام کامپیوتر و سپس آدرس IP معادل آن را وارد نمایید. سپس روی دکمه Add Host کلیک کنید.



با این کار، این رکورد به مجموعه اطلاعات DNS Server اضافه خواهد شد.

(same as parent folder)	Start of Authority (SOA)	[1], winserver2003., hostmaster.
(same as parent folder)	Name Server (NS)	winserver2003.
Reza-PC	Host (A)	192.168.1.90

بدین ترتیب هنگامی که نیاز به آدرس کامپیوتر Reza-PC داشته باشید، این DNS Server آدرس ۱۹۲.۱۶۸.۱.۹۰ را باز خواهد گرداند.

۱۷-۱۶- تست کردن DNS Server

پس از نصب DNS Server، نوبت به تست صحت کارکرد آن می شود. بدین منظور می توانیم از دستورات Ping یا NSLookUP در Command Prompt استفاده کنیم. قبل از استفاده از این دستورات، ارتباط خود را با اینترنت قطع نمایید تا عملیات Name Resolution در داخل شبکه خودتان انجام گیرد. ۱) **Ping** C:\> نام کامپیوتر ۲) **NSLookUP** C:\> نام کامپیوتر

فصل ۱۸

مفاهیم اولیه در Active Directory

۱۸-۱- آشنایی با زیرساخت های Active Directory

یک دایرکتوری (Directory) مجموعه ذخیره شده از اطلاعات درباره ی اشیایی است که به نوعی با یکدیگر مرتبط هستند. یک سرویس دایرکتوری (Directory Service) تمامی اطلاعاتی را که برای استفاده و مدیریت این اشیا لازم است، در یک محل متمرکز ذخیره نموده و بدین ترتیب نحوه ی یافتن و مدیریت این منابع را تسهیل می بخشد. یک Directory Service، زمینه ای را فراهم می آورد تا دسترسی به منابع در سطح شبکه به بهترین نحو ممکن سازمان یابد. کاربران و مدیران ممکن است که نام دقیق یک شیئ مورد نیاز (مانند چاپگر یا کاربر) را ندانند، اما با دانستن یک یا چند ویژگی از یک شیئ و با استفاده از Directory Service می توانند لیستی از اشیاء با ویژگی مورد نظر خود را جستجو کنند.

در این بخش به معرفی سرویس Active Directory پرداخته و به صورت مقدماتی با خصوصیات، اشیا موجود و اجزای آن (فیزیکی و منطقی) آشنا می شویم.

۱۸-۲- آشنایی با سرویس دایرکتوری (Active Directory)

Active Directory، یک سرویس دایرکتوری بوده که در Windows Server قرار داده شده است.

Active Directory، شامل یک دایرکتوری بوده که اطلاعات مربوط به شبکه را ذخیره می کند، علاوه بر آن دارای تمامی سرویس هایی است که اطلاعات را قابل استفاده کرده و در دسترس قرار می دهد.

۱۸-۲-۱- ویژگی های Active Directory

۱. ذخیره ی متمرکز داده (Centralized data store)

۲. مقیاس پذیری (Scalability)

۳. قابلیت توسعه (Extensibility)

۴. قابلیت مدیریت (Manageability)

۵. استفاده و تمرکز بر سیستم نام گذاری دامنه (Integration with Domain Name System)

۶. مدیریت تنظیمات سرویس گیرنده (Client configuration management)

۷. مدیریت بر مبنای سیاست (Policy-based administration)

۸. تکرار اطلاعات (Replication of information)

۹. شناسایی ایمن و انعطاف پذیر (Flexible, secure authentication and authorization)

۱۰. برنامه ها و زیر ساختار های مبتنی بر دایرکتوری (Directory-enable applications and infrastructures)

۱۱. تطبیق با سایر سرویس های دایرکتوری (Interoperability with other directory services)

۱۲. ترافیک رمز گذاری شده و امضا شده (Signed and encrypted LDAP traffic)

۱۸-۲-۲- مزایای Active Directory

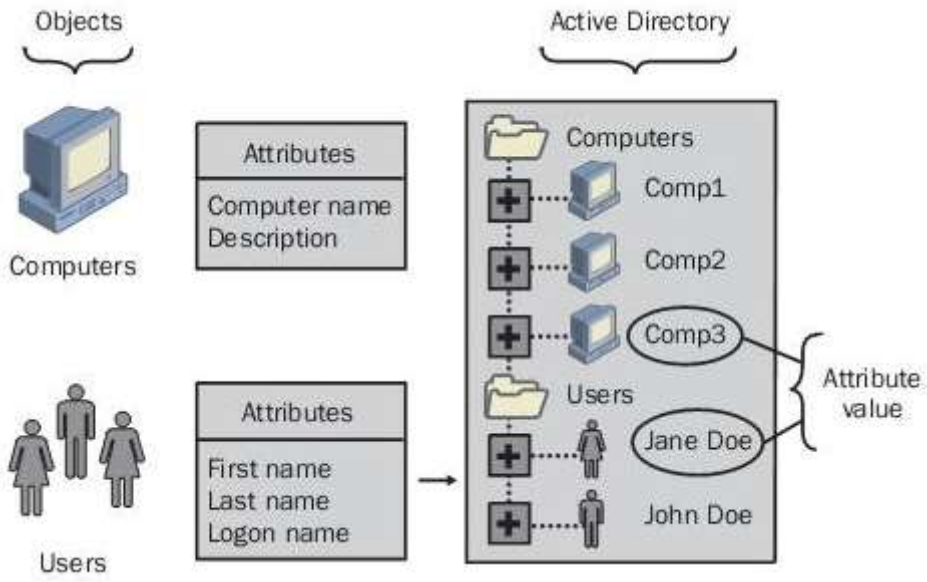
استفاده از Active Directory، دارای مزایای زیر است:

- **کاهش مجموع هزینه مالکیت:** پارامتر فوق به هزینه مالکیت یک کامپیوتر، مرتبط می گردد. هزینه فوق شامل: هزینه های مربوط به نگهداری، آموزش، پشتیبانی فنی، ارتقاء سخت افزار و نرم افزار است. Active Directory، با پیاده سازی سیاست ها باعث کاهش برخی از هزینه های فوق، می گردد. بکارگیری یک سیاست به همراه Active Directory، این امکان را فراهم می آورد که پیکربندی محیط مربوطه و نصب برنامه ها، از یک مکان مرکزی، انجام شود. بدین ترتیب زمان مربوط به پیکربندی و نصب برنامه ها بر روی هر کامپیوتر، کاهش پیدا خواهد کرد.
- **مدیریت انعطاف پذیر:** واحد های سازمانی درون یک Domain را می توان بر اساس سیاست های موجود در Active Directory، تقسیم نمود. بدین ترتیب، واحدهای سازمانی، امکان تعریف کاربرانی خاص به منظور مدیریت بخش هایی خاص از شبکه را بدست می آورند.
- **Scalability:** با استفاده از Active Directory، امکان استفاده از سرویس های دایرکتوری برای سازمان هایی با ابعاد متفاوت، فراهم می گردد.
- **تسهیل در مدیریت:** Active Directory، ابزارهای مدیریتی خاصی را ارائه که مدیران شبکه، با استفاده از آنان قادر به مدیریت منابع موجود در شبکه خواهند بود.

۱۸-۳- اشیای موجود در Active Directory

هر داده ای که در Active Directory ذخیره می شود، به صورت اشیایی (Objects) متفاوت، سازمان می یابد. یک شیئ مجموعه مجزایی از صفات است که منابع شبکه را مشخص می کند. صفات (Attributes)، خصوصیات اشیای موجود در یک دایرکتوری را شامل می شود. به عنوان نمونه صفات یک User account)) می تواند شامل نام، نام خانوادگی و نام Log on برای آن کاربر باشد. در حالی که صفات یک Computer Account ممکن است که شامل نام و مشخصات آن شیئ باشد.

بعضی از اشیا، که از آن ها به نام Container یاد می شود، خود دربردارنده اشیایی دیگرند. به عنوان مثال یک Domain، خود یک Container است که می تواند شامل اشیایی مانند حساب کاربران و کامپیوتر ها باشد. در شکل زیر، پوشه ی کاربران، یک Container بوده که دارای اشیای مربوط به حساب کاربران است.



اجزای Active Directory

برای ایجاد یک ساختار دایرکتوری، اجزای زیادی مورد نیاز است. این اجزا به دو دسته ی منطقی و فیزیکی تقسیم می شوند.

۱۸-۳-۱- اجزای منطقی

اجزای منطقی عبارتند از:

۱. دامنه ها (Domains)
۲. واحدهای سازمانی (Organizational Units)
۳. درخت ها (Trees)
۴. جنگل ها (Forests)

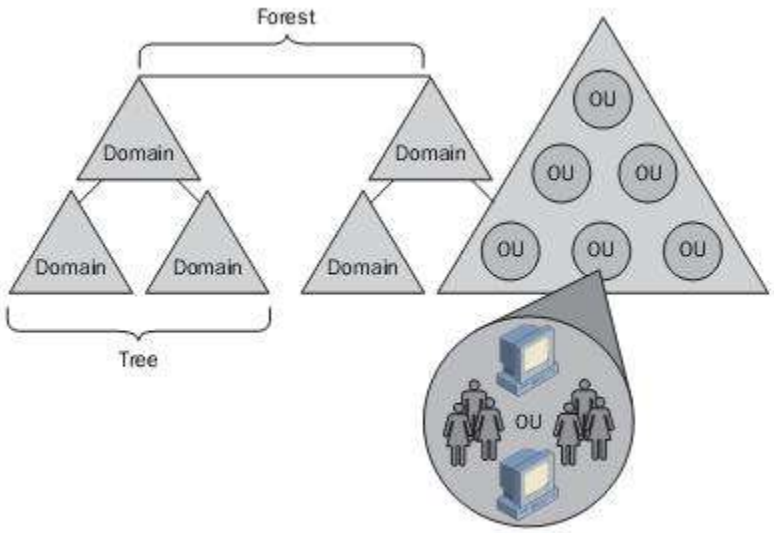
۱۸-۳-۲- اجزای فیزیکی

اجزای فیزیکی که ساختار فیزیکی Active Directory را شکل می دهند عبارتند از:

۱. سایت ها (Physical Subnets)
۲. Domain Controller ها (DC)

۱۸-۴- ساختار منطقی

در Active Directory، می توان منابع را به صورت یک ساختار منطقی سازمان داد (ساختاری که منعکس کننده ی مدل های انتزاعی سازمانی باشد). گروه بندی منطقی منابع این امکان را فراهم می آورد تا یک منبع با استفاده از نامش به سادگی پیدا شود و این امر ما را از یادآوری محل فیزیکی منبع بی نیاز می سازد. در شکل زیر رابطه ی Domainها، OU ها، treeها و Forest ها دیده می شود.



۱۸-۴-۱- دامنه – Domain

هسته ی اصلی ساختار منطقی در Active Directory، Domain یا دامنه بوده که قادر به ذخیره ی میلیون ها شیئ است. تمامی Domain ها در دو ویژگی زیر مشترک اند.

اول اینکه تمام اشیای شبکه در یک Domain قرار دارند و دوم اینکه هر Domain اطلاعات مربوط به همان Domain را دارا است.

Domain یک محدوده ی امنیتی است. دسترسی به اشیای Domain ها از طریق لیست های کنترل دسترسی یا ACL (Access Control List) میسر می شود. ACL ها شامل مجوز هایی هستند که مرتبط با اشیای مورد نظر است. این مجوز ها بیان می کنند که کدام یک از کاربران می توانند به یک شی دسترسی داشته باشند و این دسترسی از چه نوع و در چه سطحی است. در خانواده ی Windows Server، اشیاء شامل فایل ها، پوشه ها، اشتراکات، چاپگر ها و سایر اشیای Active Directory است. این نکته می بایست در نظر گرفته شود که هیچ یک از تنظیمات و سیاست های امنیتی مانند اختیارات مدیریتی، سیاست های امنیتی و ACL ها نمی توانند از یک Domain به Domain دیگر تغییر یابند. این امر بدان معنا است که یک مدیر در سطح یک Domain تنها دارای اختیاراتی است که وی را محدود به وضع سیاست ها در همان Domain می کند.

سطح عملیاتی دامنه (Domain Functional Level) که تحت عنوان حالت دامنه (Domain Mode) در Windows 2003 شناخته می شود، ویژگی های خاصی را در پهنه دامنه (Domain-Wide) و در محیط شبکه فراهم می آورد.

چهار سطح عملیاتی دامنه وجود دارد:

۱. **Windows 2000 Mixed**
۲. **Windows 2000 Native**
۳. **Windows 2003 Interim**
۴. **Windows Server 2003**

۱. سطح عملیاتی **"Windows 2000 Mixed"** به یک Domain Controller (DC) با سیستم عامل Windows Server 2003 اجازه می دهد تا با سایر DC ها در همان Domain که دارای سیستم عامل های Windows NT4، Windows 2000 و Windows server 2003 هستند ارتباط داشته باشند.
۲. سطح عملیاتی **"Windows 2000 Native"**، تنها امکان ارتباط DC های Windows 2003 با Windows 2000 را فراهم می آورد.

۳. سطح عملیاتی **"Windows 2003 Interim"** ارتباط DCهای Windows Server 2003 با DC های NT4 را ممکن می سازد.

۴. سطح عملیاتی **"Windows Server 2003"** تنها DC های ویندوز سرور ۲۰۰۳ را با یکدیگر مرتبط می سازد.

تنها در زمانی می توان سطح عملیاتی یک Domain را بالا برد که تمامی Domain Controller ها در آن Domain نسخه های مناسبی از Windows را اجرا کنند. به عنوان نمونه اگر سطح عملیاتی Domain به صورت "Windows Server 2003" باشد، در این صورت می بایست که تمامی DCها در این Domain دارای سیستم عامل Windows Server 2003 باشند.

ویژگی های یک Domain

Domain، یک گروه بندی منطقی از کامپیوتر های شبکه ای است که از یک محل مشترک به منظور ذخیره سازی اطلاعات امنیتی، استفاده می نمایند. استفاده از Domain، تمرکز در مدیریت منابع شبکه را بدنبال خواهد داشت. بدین ترتیب پس از ورود کاربران به شبکه و تائید صلاحیت آنان، زمینه استفاده از منابع به اشتراک گذاشته شده در سایر کامپیوتر های موجود در Domain، با توجه به مجوزهای تعریف شده، فراهم می گردد. Domain، در مفهوم مشابه Workgroup بوده ولی امکانات و ویژگی های بمراتب بیشتر و مفید تری را ارائه می نماید:

- **Single logon**: با استفاده از Domain، فرآیند ورود به شبکه صرفاً یک مرتبه انجام و کاربران قادر به استفاده از منابع متفاوت موجود در شبکه شامل: فایل ها، چاپگر ها و برنامه ها، خواهند بود. Account مربوط به تمامی کاربران در یک مکان متمرکز، ذخیره می گردد.
- **Single User Account**: کاربران یک Domain، صرفاً از یک Account به منظور دستیابی به منابع موجود بر روی کامپیوتر ها، استفاده خواهند کرد (بر خلاف Workgroup که نیازمند یک account مجزا به منظور دستیابی به هر یک از کامپیوتر ها است).
- **مدیریت متمرکز:** با استفاده از Domain، امکان مدیریت متمرکز فراهم خواهد شد. Account مربوط به کاربران و منابع اطلاعاتی موجود، از طریق یک نقطه متمرکز، مدیریت خواهد شد.
- **Scalability**: استفاده از Domain، امکان گسترش و توسعه در شبکه را افزایش خواهد داد. روش دستیابی کاربران به منابع و نحوه مدیریت منابع در یک شبکه بسیار بزرگ مشابه یک شبکه کوچک خواهد بود.

مزایای استفاده از Domain

استفاده از Domain، دارای مزایای زیر است:

- **سازماندهی اشیاء:** اشیاء موجود در یک Domain را می توان بر اساس واحدهای موجود در یک سازمان، سازماندهی نمود. یک واحد سازماندهی شده شامل مجموعه ای از اشیاء در یک Domain است. اشیاء، نشان دهنده عناصر فیزیکی موجود در یک شبکه بوده و می توانند به یک و یا بیش از یک Domain مرتبط گردند. کاربران، گروه هایی از کاربران، کامپیوتر ها، برنامه ها، سرویس ها، فایل ها و لیست های توزیع شده نمونه هایی در این زمینه می باشند. مثلاً یک Domain در شبکه مربوط به یک سازمان، می تواند به منظور تسهیل در مدیریت منابع موجود در شبکه، منابع هر یک از دپارتمان های موجود در سازمان را در یک واحد، سازماندهی نماید. هر واحد، می تواند توسط کاربران خاصی در دپارتمان مربوطه مدیریت گردد. بدین ترتیب مدیر شبکه قادر به مدیریت گروه هایی از واحدها در مقابل منابع انفرادی، خواهد بود.
- **مکان یابی آسان اطلاعات:** به موازات نشر (تعریف و پیکربندی) یک منبع، امکان دستیابی آن از طریق لیستی از اشیاء یک Domain، برای کاربران فراهم و بدین ترتیب مکان یابی یک منبع به سادگی انجام و زمینه استفاده از آن فراهم خواهد شد. مثلاً در صورتی که چاپگری در یک Domain نصب شده باشد، کاربران قادر به دستیابی به آن از

طریق لیستی از اشیاء موجود در Domain مربوطه خواهند بود. در صورتی کـه چـاپگر در Domain مربوطـه تعریـف نشده باشد، کاربران شبکه جهت استفاده از آن می بایست از محل نصب آن آگاهی داشته باشند.

- **دستیابی آسان و موثر:** تعریف و بکارگیری یک سیاست گروهی در ارتباط با یک Domain، نحوه دستیابی کـاربران به منابع تعریف شده در Domain را مشخص می نماید. بدین ترتیب استفاده از منابع به همـراه رویکردهـای امنیتـی، یکپارچه می گردد.
- **تفویض اختیار:** با استفاده از Domain، امکان واگذاری مسئولیت مربوط به مدیریت اشیاء در تمام Domain و یـا در بخش هایی خاص، فراهم می گردد.

ساختار Domain

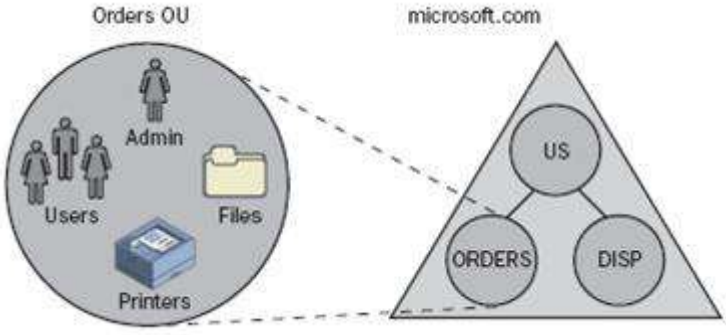
هر Domain توسط یک کنترل کننده Domain، مدیریت می گردد. به منظور تسهیل در مدیریت چندین Domain، می توان Domain ها را در ساختار هایی با نام درخت (Tree) و جنگل (Forest)، گروه بندی کرد.

کنترل کننده دامنه (DC)

کامپیوتری که برروی آن سرویس دهنده ویندوز سرور اجراء و مدیریت Domain را برعهده می گیرد، کنترل کننـده Domain نامیده می شود. کنترل کننده Domain، تمام عملیاتی امنیتی مرتبط با کاربران و Domain را مدیریت می نماید.

۱۸-۴-۲- واحدهای سازمانی - OUs (Organization Units)

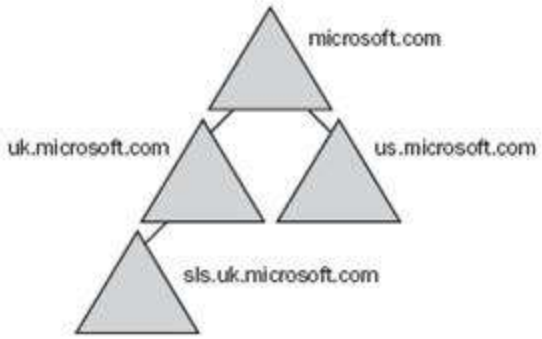
OU خود یک Container بوده که اشیای یک دامنه (Domain) را در گروه های مدیریتی سازمان دهـی مـی کنـد. یـک OU برای اعمال و اجرای وظایف مدیریتی (مانند مدیریت منابع و کاربران) به کار رفته و می تواند شامل اشیایی مانند حساب هـای کاربران، گروه ها، کامپیوتر ها، چاپگر ها، برنامه ها، فایل های به اشتراک گذاشته شده و حتی سایر OU ها از همـان Domain باشد. ساختار سلسله مراتبی یک OU در یک Domain، مستقل از ساختار سلسله مراتبی OU درDomain هـای دیگـر اسـت. می توان با اضافه کردن یک OU در داخـل OU دیگـر (Nesting)، مـدیریتی سلسـله مراتبـی را سـازمان داد. در شـکل زیـر، Domain با نام Microsoft.com منعکس کننده ی سازمانی بوده که دارای سه واحد سازمانی است : US، Orders و Disp. Orders و Disp در واحد سازمانی US آشیانه ای شده اند. به صـورت پـیش فـرض تمـامی اشـیای فرزنـد (OUهـای Disp و Order) مجوزهای خود را از والدین به ارث می برند (US OU). ایجاد مجـوز در سـطوح بـالاتر و اسـتفاده از امکانـات وراثـت، وظایف مدیریتی را کاهش می دهد.



۱۸-۴-۳- درخت ها - Trees

یک درخت (Tree)، سازمان دهی یا گروه بندی منطقی یک یا چند دامنه بوده که از طریق ایجاد یا اضافه کردن چند دامنه ی فرزند (Child Domain) به دامنه ی پدر (Parent Domain) فعلی به وجود می آید. دامنه ها در یک درخت، دارای یک فضای اسمی (Contiguous Namespace) یا ساختار نامی سلسله مراتبی مشترک هستند. بر اسـاس اسـتانداردهای DNS، نـام یـک دامنه ی فرزند، ترکیبی از نـام خـود دامنـه ی فرزنـد بـه همـراه نـام دامنـه ی پـدر اسـت. در شـکل زیـر، Domain بـا نـام Microsoft.com به عنوان دامنه ی والد و Domain هـای us.microsoft.com و uk.microsoft.com دامنـه هـای فرزنـد آن

هستند. علاوه بر آن خود دامنه ی uk.microsoft.com دارای یک دامنه ی فرزند با نام sls.uk.microsoft.com است (به روند دنباله دار نام دامنه ها دقت کنید).



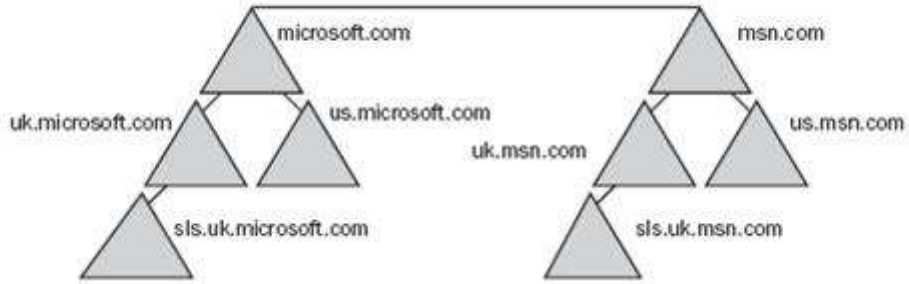
۱۸-۴-۴- جنگل ها – Forests

یک جنگل (Forest) دسته بندی یا سازماندهی سلسله مراتبی از یک یا چند درخت (Domain Tree) کاملاً مستقل و مجزا از هم است. یک جنگل دارای ویژگی هایی است:

۱- درخت ها در یک جنگل با توجه به دامنه هایشان، دارای ساختار نامی متفاوت هستند.

۲- دامنه ها در یک جنگل به صورتی کاملاً مستقل از هم عمل می کنند، ولی یک جنگل امکان ارتباط در تمامی سازمان را برقرار می سازد.

در شکل زیر دو درخت microsoft.com و msn.com از یک جنگل دیده می شوند. می توان مشاهده کرد که فضای نامی در هر درخت دنباله دار است.

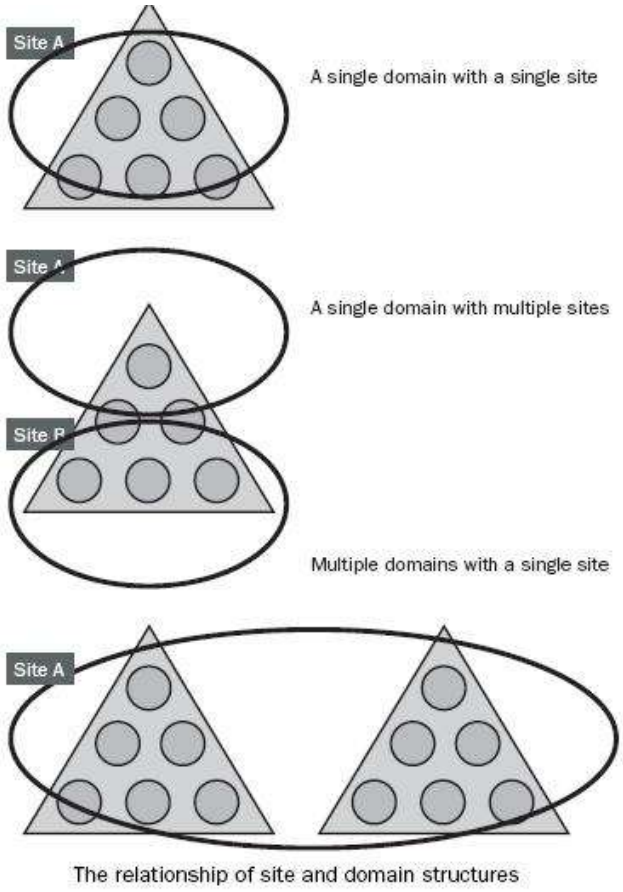


سطح عملیاتی جنگل (Forest Functional Level)، ویژگی های خاصی را در سطح جنگل و در محیط شبکه فراهم می آورد (Forest-wide Active Directory Features).

۱۸-۵- ساختار فیزیکی

۱۸-۵-۱- سایت ها (Sites)

یک سایت اجتماع یک یا چند زیر شبکه IP (Subnet) است که به وسیله ی یک اتصال فیزیکی **مطمئن و سریع** به هم مرتبط شده اند تا بتوان تا آنجا که ممکن است در جهت بهبود ترافیک شبکه اقدام کرد. سایت ها تنها شامل اشیای کامپیوتری و ارتباطی هستند که به منظور تنظیم چگونگی تکرار در سایت (Replication) به کار گرفته شده اند. همان گونه که در شکل زیر نشان داده شده است، یک دامنه مجزا می تواند شامل یک یا بیش از یک سایت (از لحاظ جغرافیایی) باشد، و یک سایت مجزا می تواند شامل حساب های کاربران و کامپیوتر هایی باشد که متعلق به چندین دامنه هستند.



The relationship of site and domain structures

۱۸-۵-۲- DC (Domain Controller)

یک Domain Controller، کامپیوتری است که دارای سیستم عامل Windows Server باشد و یک نسخه از دایرکتوری دامنه (Local Domain Database) یا Replica را در خود ذخیره کند. هر دامنه می تواند بیش از یک Domain Controller داشته باشد. یک Domain Controller تنها می تواند به یک دامنه سرویس دهد. یک DC وظیفه ی شناسایی کاربرانی را که تلاش برای Log On به دامنه دارند، را بر عهده دارد. علاوه بر آن سیاست های امنیتی برای یک دامنه را نیز تنظیم و حفظ می کند.

۱۸-۶- درک مفاهیم Active Directory

در خانواده ی ویندوز سرور ۲۰۰۳، با مفاهیم جدیدی در ارتباط با Active Directory روبرو می شویم. این مفاهیم شامل موارد زیر است:

۱. تکرار (Replication)
۲. ارتباطات مطمئن (Trust Relationships)
۳. سیاست های گروهی (Group Policies)

اکنون به توضیح موارد فوق می پردازیم:

۱۸-۶-۱- تکرار یا Replication

کاربران و سرویس ها می بایست در هر زمانی و از هر کامپیوتری در Domain، به اطلاعات دایرکتوری دسترسی داشته باشند. انعکاس (Replication) این امر را تضمین می نماید که هر تغییری در یک Domain controller، در سایر DCها از همان Domain نیز منعکس می شود. اطلاعات دایرکتوری در Domain controller های داخل و بین سایت ها تکرار می شود.

چه اطلاعاتی تکرار می شود؟

آنچه که در دایرکتوری ذخیره می شود (در فایل Ntds.dit) به صورت منطقی به چهار دسته تقسیم می شود. به هر یک از این دسته های اطلاعاتی، لفظ Directory Partition اطلاق می گردد. یک پارتیشن دایرکتوری را با عنوان متن نامی (Naming Context) نیز می شناسند. دایرکتوری دارای پارتیشن های زیر است:

۱. **Schema Partition:** این پارتیشن اشیایی را مشخص می سازد که می توانند در دایرکتوری ساخته شوند. علاوه بر آن، این پارتیشن ویژگی ها و صفات این اشیا را نیز مشخص می سازد. این اطلاعات و داده ها در کل یک Forest مشترک بوده و در تمامی DC های موجود در یک Forest تکرار می شود.
۲. **Configuration Partition:** این پارتیشن ساختار منطقی چیدمان Active Directory را بیان می دارد و شامل داده هایی درباره ی ساختار Domain و یا توپولوژی تکرار است. این داده ها نیز در تمامی Domain های موجود در یک Forest مشترک بوده و در تمامی DC های موجود در آن جنگل تکرار می شوند.
۳. **Domain Partition:** این پارتیشن تمامی اشیای موجود در یک Domain را تعریف می کند. این داده ها و اطلاعات مخصوص به یک Domain بوده و منحصر به فرد در همان Domain است و بنابراین در دیگر Domain های موجود در یک Forest تکرار نخواهد شد.
۴. **Application Directory Partition:** این پارتیشن شامل اطلاعات پویای کاربردی است. ذخیره ی این اطلاعات در این پارتیشن موجب کنترل حوزه ی تکرار و محل نسخه های تکرار (Replica) می گردد و این امر کوچکترین تأثیر نا مطلوبی در کارآیی شبکه را به دنبال نخواهد داشت. این پارتیشن می تواند هر نوع شی را دارا باشد (به غیر از اشیای امنیتی که شامل کاربران گروه ها و کامپیوتر ها می باشد.) بدین ترتیب داده می تواند به صورتی مشخص به DC هایی هدایت شود که برای کارهای مدیریتی در نظر گرفته شده اند و این امر ترافیک غیر ضروری تکرار (Replication) را کاهش می دهد.

یک Domain Controller، موارد زیر را ذخیره کرده و تکرار می نماید:

۱. داده ی موجود در Schema Partition در سطح Forest
۲. داده ی موجود در Configuration Partition، به تمامی Domain ها در سطح یک Forest
۳. داده ی موجود در Domain partition (تمامی اشیای دایرکتوری و مشخصات آن ها) برای همان Domain. این داده ها در تمامی Domain Controller های اضافی موجود در آن Domain تکرار خواهد شد. به منظور یافتن بهینه ی اطلاعات، بخشی از نسخه ی تکرار (Replica) که شامل صفاتی از تمام اشیایی است که به صورتی دائمی در Domain مورد استفاده قرار می گیرند، در کاتالوگ سراسری (Global Catalog) نیز تکرار می گردد. کاتالوگ سراسری محلی مرکزی برای نگهداری اطلاعات در مورد اشیا در یک درخت یا جنگل است.

یک Global Catalog اطلاعات زیر را ذخیره و تکرار می نماید:

۱. داده های موجود در Schema Partition برای یک Forest
۲. داده های موجود در Configuration Partition برای تمامی Domain ها در یک Forest
۳. بخشی از Replica که شامل صفاتی از تمام اشیای دایرکتوری است که معمولاً در یک Forest مورد استفاده قرار می گیرند (این اطلاعات تنها بین Global Catalog ها تکرار می شود).
۴. تمامی Replica که شامل کل صفات تمام اشیای دایرکتوری در Domainهایی است که کاتالوگ سراسری در آن قرار دارد.

اطلاعات چگونه منعکس می شود؟

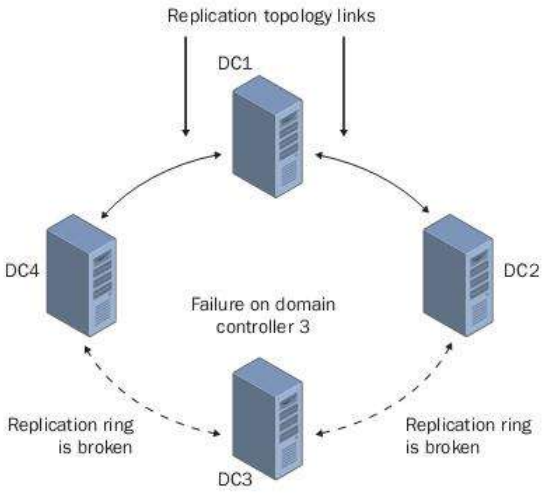
Active Directory اطلاعات را به دو صورت منعکس می کند:

- **IntraSite (در داخل یک سایت)**
- **InterSite (بین سایت ها)**

انعکاس در داخل سایت (IntraSite Replication)

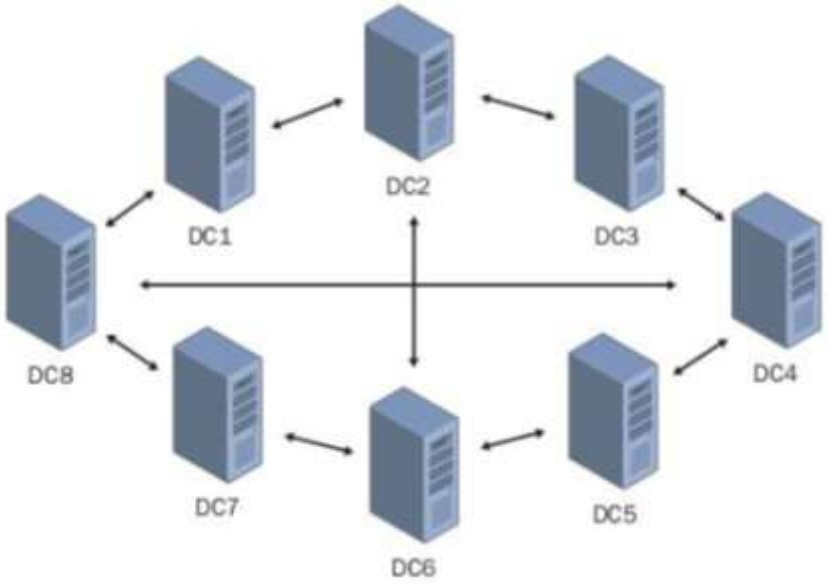
در داخل یک سایت، سرویسی از ویندوز سرور ۲۰۰۳ تحت عنوان Knowledge Consistency Checker که به اختصار آن را KCC می نامیم، به صورت خودکار یک توپولوژی برای تکرار در میان Domain controllerها در همان دامنه و با استفاده از یک ساختار حلقه ایجاد می کند. KCC یک پروسه ی خودکار است که در تمامی DC ها اجرا می شود. توپولوژی اعمال شده مسیری برای به روز رسانی های دایرکتوری فراهم می آورد تا از یک DC به DC دیگر جریان یابد و این انتقال تا زمانی ادامه می یابد که DC های موجود در یک سایت به روز رسانی های دایرکتوری را دریافت نمایند. KCC تصمیم می گیرد که کدام یک از سرور ها برای انجام عمل انعکاس با یکدیگر مناسب تر هستند و سایر DC ها را به عنوان شرکای انعکاس آن ها در نظر می گیرد. این تصمیم گیری بر اساس مواردی چون نحوه ی اتصال، سابقه ی انعکاس موفق و بر مبنای تطابق با نسخه های انعکاس جزئی و یا کامل است. هر DC می تواند بیش از یک شریک برای انعکاس داشته باشد. بعد از آن KCC اشیای ارتباطی را می سازد که ارتباط میان شرکای انعکاس را نمایش خواهد داد.

ساختار حلقه تضمین می کند که حداقل دو مسیر انعکاس از یک DC به DC دیگر وجود دارد. به همین دلیل اگر یکی از DC ها از کار بیفتد، عمل انعکاس (Replication) به سایر DC ها ادامه خواهد یافت. شکل زیر توپولوژی انعکاس در داخل سایت را نشان می دهد.



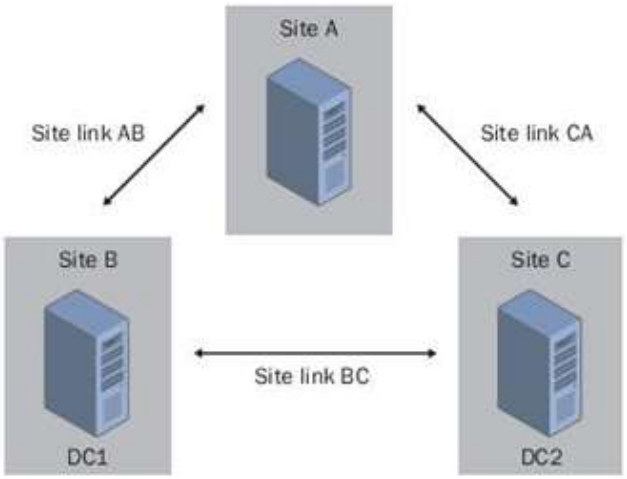
KCC توپولوژی انعکاس در داخل سایت را هر ۱۵ دقیقه یکبار بررسی کرده و از کارکرد آن اطمینان حاصل می کند. با اضافه یا خارج کردن یک DC از شبکه، KCC توپولوژی انعکاس را مجددا پیکربندی می کند تا این تغییرات در آن منعکس شود.

هنگامی که بیش از **هفت** Domain Controller به یک سایت اضافه می شوند، KCC اشیای ارتباط اضافی را در ساختار حلقه دخیل می کند تا این اطمینان حاصل شود که اگر تغییری در هر یک از DC ها ایجاد شود، هیچ یک از DC ها بیش از سه Hop (گام) از DC دیگر فاصله نداشته باشند. این ارتباطات بهینه به صورت تصادفی ایجاد می شوند و الزامی برای ساخت آنها در هر DC نیست. شکل زیر این مورد را نشان می دهد.



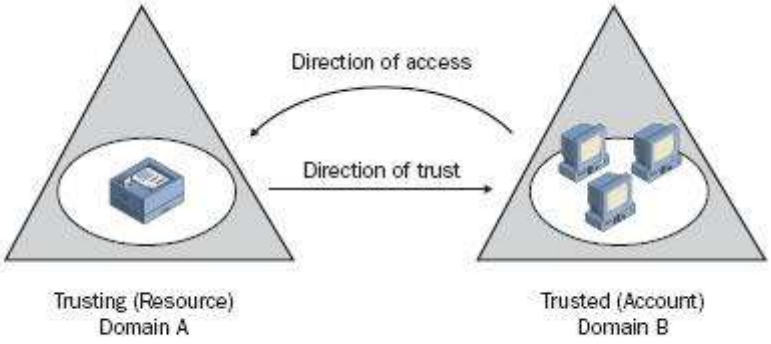
انعکاس بین سایت ها (InterSite Replication)

به منظور اطمینان از برقراری انعکاس میان سایت ها، می بایست که سایت ها بـه صـورت دسـتی و از طریـق ایجـاد اتصـالات سایتی (Site Link) به هم مرتبط شوند. اتصالات سایتی ارتباطات شبکه را نشان داده و وقوع انعکاس را ممکن می سازند. یک KCC مجزا در یک سایت تمامی ارتباطات میان سایت ها را برقرار می سازد. این امر در شکل زیر نشان داده شده است.



۱۸-۶-۲- ارتباطات مطمئن (Trust Relationships)

یک Trust، اتصالی میان دو دامنه است که در آن دامنه ی اعتماد کننده (Trusting Domain)، اطلاعات مربوط به دسترسی و شناسایی را از دامنه ی مورد اعتماد (Trusted Domain) کسب می کند. دو دامنه وجود دارند که موجب برقراری یـک رابطـه ی مطمئن و یا یک Trust می شوند: دامنه ی اعتماد کننده (Trusting) و دامنه ی مورد اعتماد (Trusted). دامنـه ی اعتمـاد کننده، دامنه ای است که منابع را در اختیار داشته و به سایر دامنه ها برای استفاده از این منابع اعتمـاد دارد. دامنـه ی مـورد اعتماد در حقیقت استفاده کننده از منابع است. این مسئله در شکل زیر بهتر نمود می یابد.



Trusting and trusted domains linked with a one-way trust

Trust ها ویژگی های زیر را دارا هستند:

۱. **چگـونگی ایجـاد (Method Of Creation)**: Trust هـا مـی تواننـد بـه صـورت صـریح (Explicitly) یـا ضـمنی (Implicitly) ساخته شوند. هیچ Trustی نمی تواند به هر دو صورت ساخته شود.

۲. **ترانهادگی (Transitivity)**: یـک Trust ترانهـاده یعنـی آنکـه اگـر Domain A بـه Domain B و Domain B بـه Domain C اعتماد یا Trust دارد، آنگاه Domain A نیز به Domain C اعتماد می کند. یک Trust غیر ترانهاده یعنی آن کـه اگـر Domain A بـه Domain B و Domain B بـه Domain C اعتمـاد یـا Trust دارد، بـین Domain A و Domain C هیچ ارتباط مطمئن یا Trust برقرار نیست.

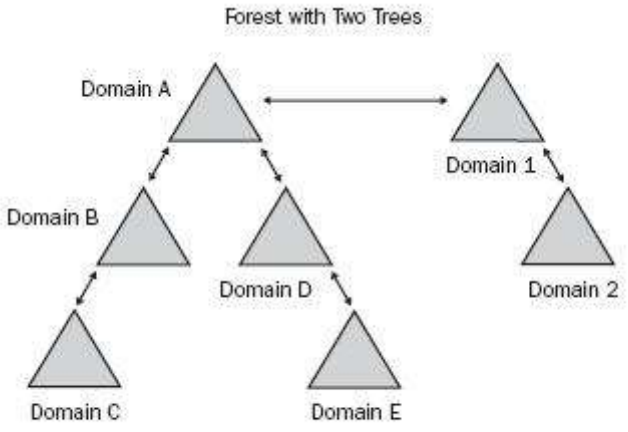
۳. **جهت (Direction)**: Trust ها می توانند یک طرفه(One-Way) یا دو طرفه (Two-Way) باشند. در یک اعتماد یـک طرفه، Domain A به Domain B، Trust دارد. در یک Trust دو طرفه اگر Domain A به Domain B اعتماد داشته باشد، آنگاه Domain B نیز به Domain A اعتماد دارد.

ویندوز سرور ۲۰۰۳ از انواع Trust هایی که در زیر آمده است پشتیبانی می کند.

- Parent-Child Trust
- Tree-Root Trust
- Shortcut Trust
- External Trust
- Forest Trust
- Realm Trust

Parent-Child Trust با ایجاد یک درخت و به صورت اتوماتیک میان تمامی دامنه های موجود در آن درخت به وجـود مـی آید. با اضافه شدن یک دامنه ی جدید به یک درخت، پروسه ی ایجاد اتوماتیک Trust صورت می پـذیرد. ایـن نـوع Trust دو طرفه و ترانهاده است.

Tree-Root Trust نیز به صورت اتوماتیک و با اضافه شدن یک درخت به ساختار جنگـل (A New Root Tree) برقـرار مـی شود شکل زیر این Trustها را نشان می دهد. این نوع Trust نیز دو طرفه و دارای خاصیت ترانهادگی است.



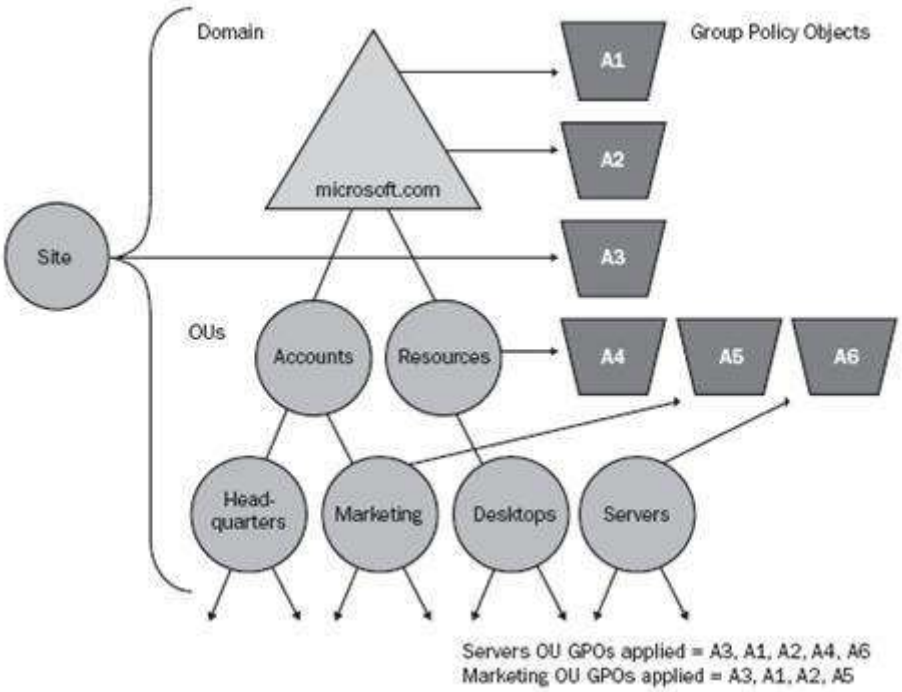
Domain structure showing tree-root and parent-child trusts

۱۸-۶-۳- سیاست های گروهی (Group Policies)

سیاست های گروهی، مجموعه ای از تنظیمات برای کاربران و کامپیوتر ها است که می تواند به کامپیوتر ها، سایت ها، دامنه ها و OUها اعمال گردد تا بدین ترتیب عملکرد کاربران بهتر مشخص گردد.GPO ها مجموعه ای از سیاست های گروهی تنظیم شده است. برای معلوم کردن تنظیمات Desktop برای گروهی از کاربران مشخص، اشیای سیاست گروهی (Group Policy Objects or GPOs) ساخته می شوند. هر کامپیوتر با سیستم عامل ویندوز دارای یک GPO داخلی بوده (Local GPO) و علاوه بر آن می تواند با یک سری از سیاست های غیر محلی (مبتنی بر Active Directory) مرتبط گردد.GPO های غیر محلی بر GPO داخلی اولویت می یابند.GPO های غیر محلی یا به کاربران (بدون در نظر گرفتن کامپیوتری که به آن Log On می کنند) و یا به کامپیوتر ها (بدون در نظر گرفتن کاربری که به آن Log On می کنند) اعمال می گردد و مربوط به اشیای خاص Active Directory (دامنه ها، سایت ها و OU ها) است. این نوع از سیاست ها به صورت سلسله مراتبی و از گروه با کمترین محدودیت (Site) به گروه با بیشترین محدودیت (OU) اعمال می شود. در حقیقت چگونگی و ترتیب اعمال به صورتی که در زیر آمده، است:

۱. **Local GPO**: هر سیستم عامل ویندوز تنها دارای یک سیاست گروهی است که به صورت محلی ذخیره شده است.
۲. **GPOs Linked To Sites**: هر GPO که به یک سایت مرتبط باشد در مرحله ی بعد اعمال می شود. این اعمال برای تمامی سیاست های مرتبط با یک سایت همزمان صورت می گیرد و مدیر یک شبکه تعیین کننده ی ترتیب اعمال است.
۳. **GPOs Linked to Domains**: اولویت اعمال این دسته از سیاست ها نسبت به دو مورد اول بیشتر است. اما اولویت اعمال چندین سیاست مربوط به یک دامنه را مدیر شبکه تعیین می کند.
۴. **GPOs linked to OUs**: GPO هایی که در بالای ساختار سلسله مراتبی یک OU قرار دارند زودتر اعمال می شوند. پس از آن، GPO های مربوط به OU های فرزند اعمال شده و در نهایت GPO های مربوط به OU شامل کاربران و کامپیوتر ها اعمال می شود. در هر سطح از OU می توان بیش از چند GPO را اعمال نمود (حتی می توان هیچ GPO را اعمال نکرد).

شکل زیر چگونگی اعمال سیاست گروهی برای دو OU ی نمونه ی Server و Marketing را نشان می دهد.


Domain
Group Policy Objects
A1
A2
A3
microsoft.com
Site
OUs
Accounts
Resources
A4
A5
A6
Head-quarters
Marketing
Desktops
Servers
Servers OU GPOs applied = A3, A1, A2, A4, A6
Marketing OU GPOs applied = A3, A1, A2, A5

فصل ۱۹

نصب و راه اندازی Active Directory

۱۹-۱- نصب Active Directory

از جمله امکانات قدرتمند Windows Server 2003 Advanced، Active Directory است که امکان مدیریت کاربران، کامپیوتر ها، گروه ها و بطور کلی تمامی عناصر موجود در یک شبکه را فراهم می کند. در واقع اگر بخواهیم کامپیوتری به یک سرور واقعی تبدیل شود و بتواند یک دامنه را کنترل کند (Domain Controller)، بایستی Active Directory را روی آن نصب کرد. (البته نباید اینگونه تصور نمود که Active Directory تمامی مشکل یک مدیر شبکه را حل می نماید). با استفاده از قابلیت های Active Directory می توان مشخص کرد کدام User با کدام Computer تحت کدام Domain به چه کاری بپردازد. یعنی میزان دسترسی آن به منابع موجود در شبکه چه مقدار باشد و تا چه میزان در این کار اختیار دارد و اجازه دسترسی دارد (مثلاً امکان نوشتن یا جابجا نمودن و حتی امکان دسترسی به دیگر کاربران و اینکه خود در چه سطحی از مدیریت نمودن شبکه قرار بگیرد). با استفاده از قابلیت Active Directory در Windows Server 2003 Advanced مدیریت شبکه بسیار آسان است.

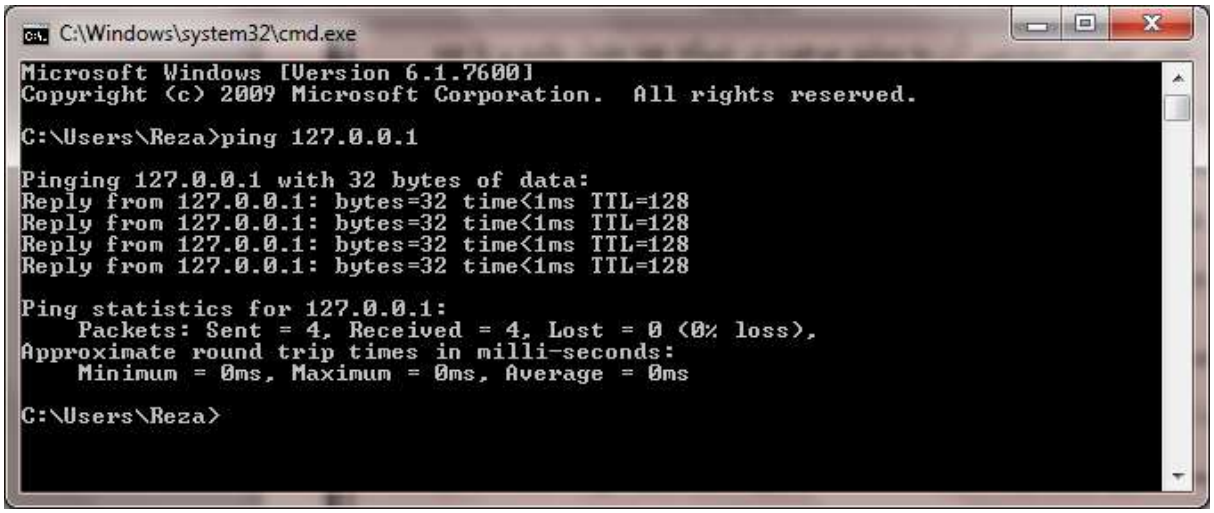
چند نکته مهم در استفاده از Active Directory:

۱. اولین عاملی که باید در Active Directory مد نظر داشت این است که سیستم فایل ما باید از نوع NTFS باشد تا امکان استفاده ازActive Directory را داشته باشیم. بنابراین اگر سیستم فایل ما از نوع FAT باشد، ابتدا باید نوع سیستم فایل درایو مورد نظر را به NTFS تبدیل کنیم. برای این کار از دستور Convert موجود در Command Prompt استفاده کنیم.

Run➔ CMD➔ Convert D: /fs:NTFS
درایو مورد نظر :D می باشد.

۲. صحت تنظیمات کارت شبکه و پروتکل کامپیوتر مورد نظر نیز کنترل شود. برای اینکار در Command Prompt دستور زیرا را وارد کنید. نتیجه کار باید مانند شکل زیر باشد:

C:\> Ping 127.0.0.1

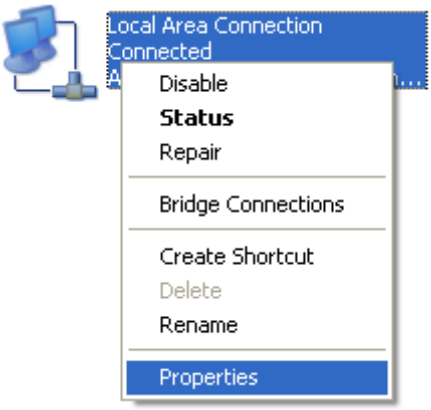


۳. سپس باید DNS Server را نصب کنید. وظیفه DNS Server تبدیل اسامی Host به آدرس IP است. توجه نمایید که در صورت عدم نصب DNS Server، سرور و Active Directory قادر به انجام وظایف خود نیست. برای آشنایی با DNS Server و نحوه نصب آن به فصل DNS Server مراجعه فرمایید.

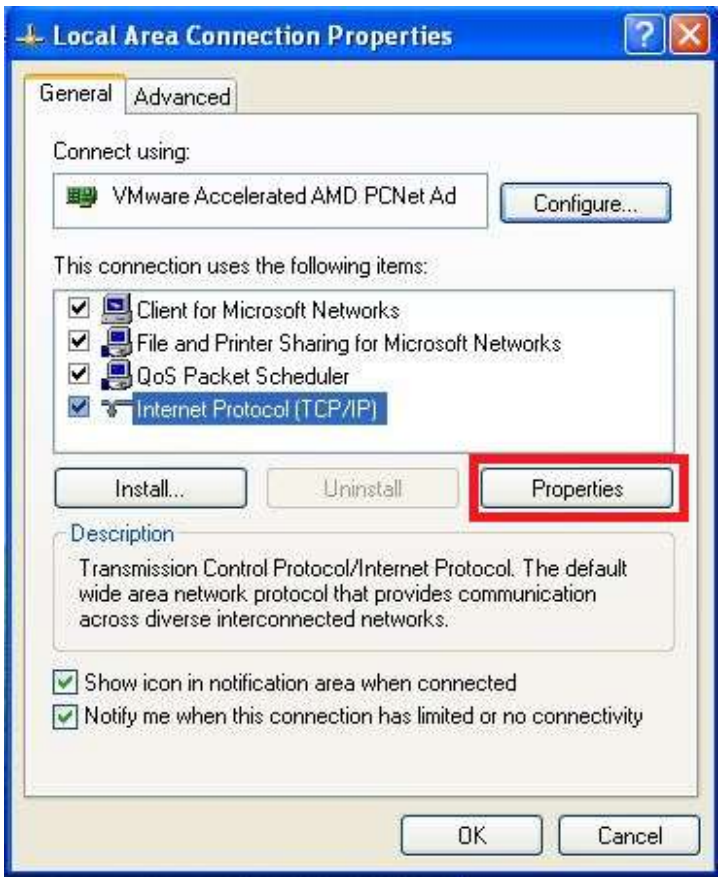
۴. IP Address را باید حتما به صورت دستی (ایستا) تنظیم کنیم. زیرا IP سرور نباید متغیر باشد. برای اینکار وارد مسیر زیر شوید:

Control Panel ➔ Network Connections

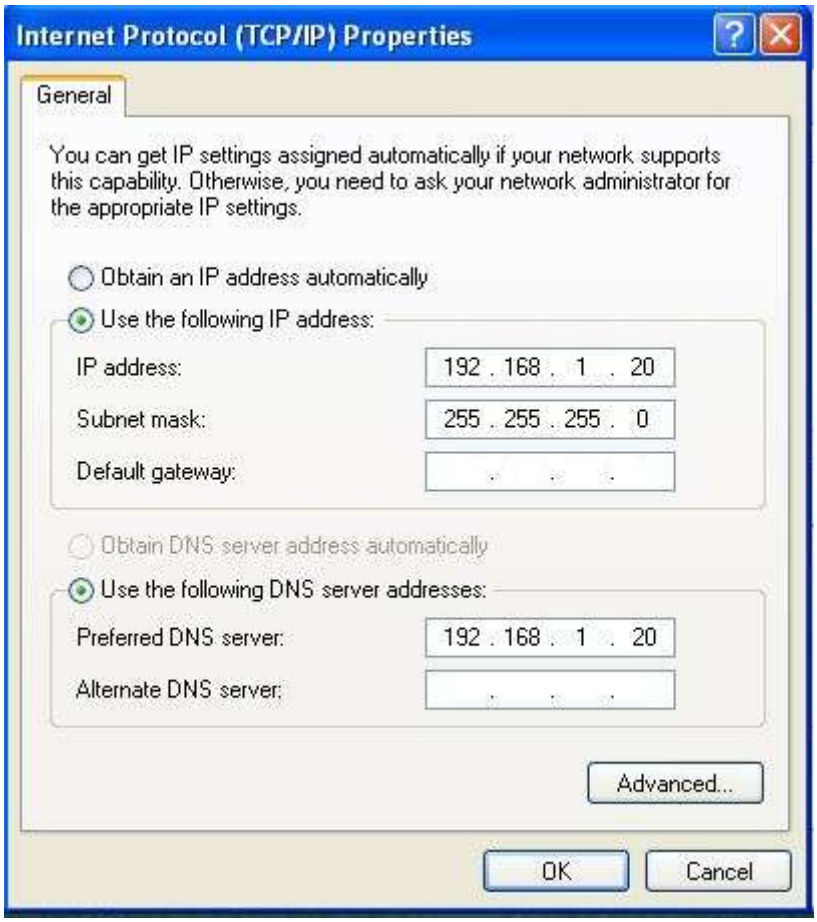
روی Local Area Network راست کلیک کرده و Properties را انتخاب نمایید.



در صفحه باز شده، گزینه Internet Protocol (TCP/IP) را انتخاب کرده و سپس روی دکمه Properties کلیک نمایید.



در صفحه باز شده، مانند شکل زیر، آدرس IP را به صورت دستی تنظیم کنید. در قسمت Preferred DNS نیـز آدرس DNS Server که نصب کرده اید را وارد نمایید. در نهایت روی دکمه OK کلیک کنید.



۵. بهتر است که در شبکه Client های خود را از خانواده Windows NT (XP , 2000 Pro , NT Work Station) باشد. در اینصورت به بهترین وجه می توان امنیت شبکه و کامپیوتر های آن را تامین نمود.

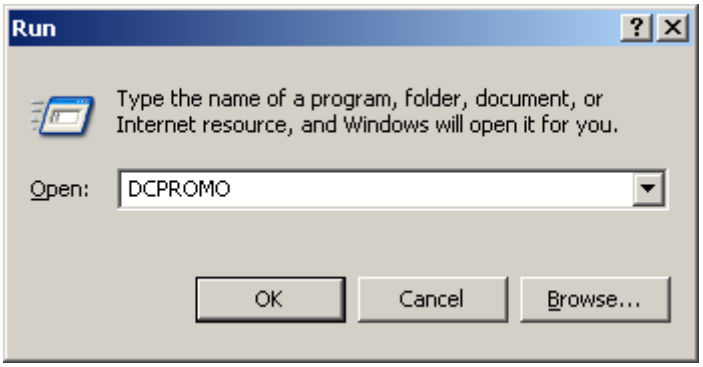
۶. باید حداقل 1 GB فضای خالی داشته باشیم.

در صورتی که موارد فوق را به درستی انجام داده باشیم، سیستم ما آماده نصب Active Directory می باشد. درصورت نصب Active Directory، سرور ما تبدیل به یک Domain Controller خواهد شد.

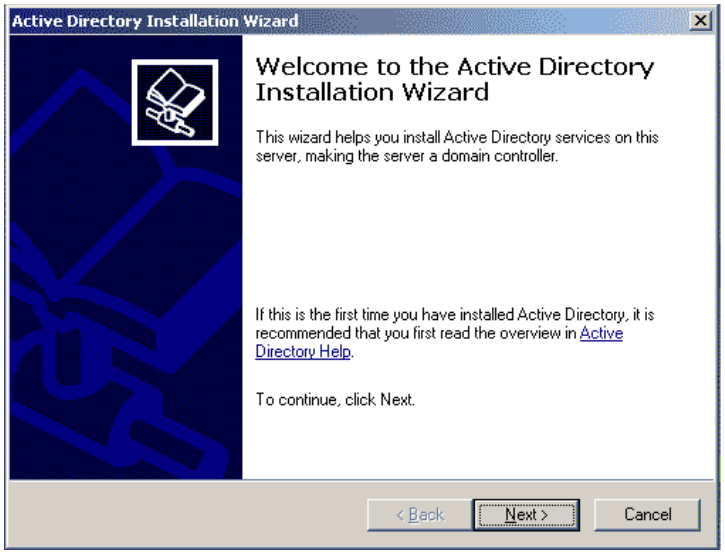
قابل ذکر است که این طریق نصب، طریقه نصب به صورت حرفه ای می باشد و در صورتی که بخواهید می توانید به صورت خیلی آسان از طریق پنجره ی Manage Your Server از داخل Administrative Tools این کار را به راحتی تمام و به صورت Wizard انجام دهید.

برای شروع نصب منوی Start را باز کرده و در RUN عبارت زیر را تایپ می کنیم: DCPROMO

DCPromo مخفف Domain Controller Promotion و به معنای ارتقای کنترل کننده دامنه میباشد.

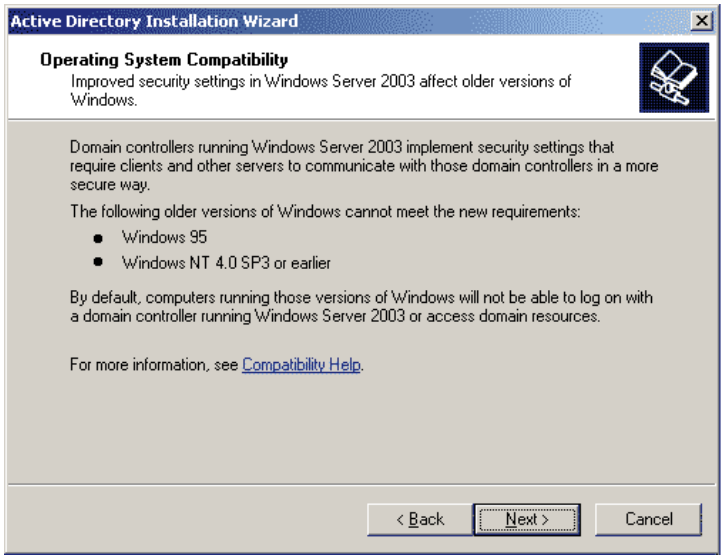


در ابتدا صفحه خوش آمد گویی مبنی بر نصب Active Directory ظاهر خواهد شد.



بر روی دکمه ی Next کلیک می کنیم و به صفحه بعدی هدایت می شوید.

در این صفحه به شما هشدار می دهد که در صورتی که در شبکه خود کامپیوتر هایی با سیستم عامل های Win 95 و یا Win NT SP 3.0 یا قدیمی تر داشته باشید، نمی توانند به DC وصل شوند و عملیات Login را انجام دهند و نمی توانند از منابع به اشتراک گذاشته شده در شبکه استفاده کنند.



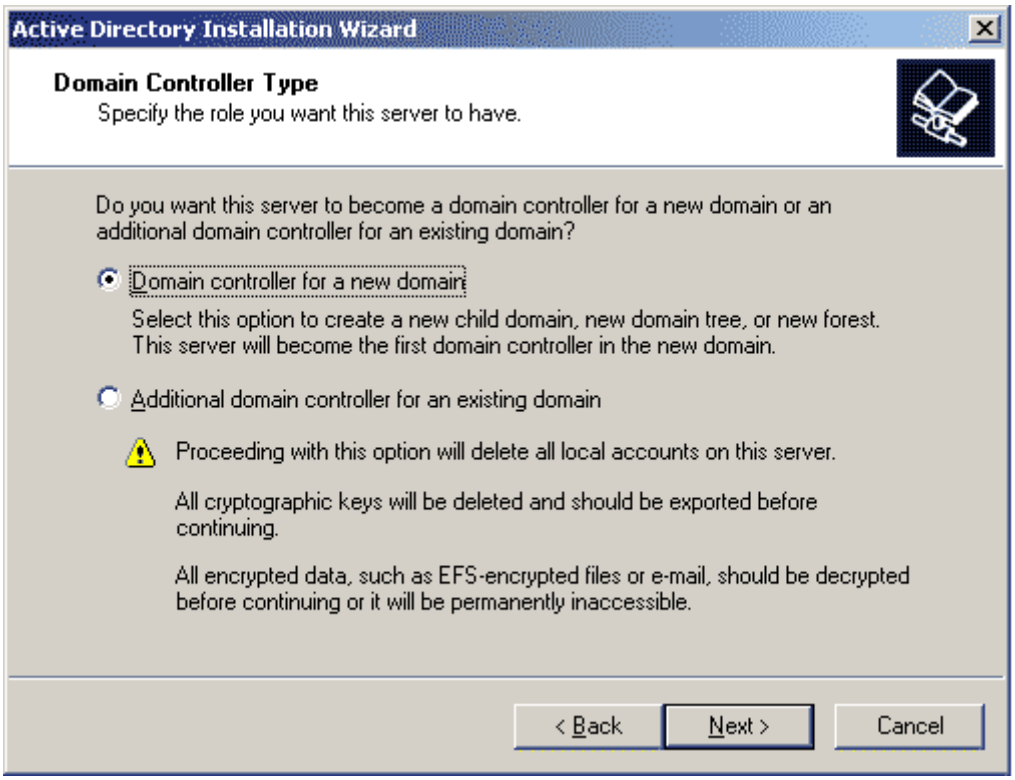
بر روی دکمه Next کلیک کرده و به صفحه بعدی بروید.

در این صفحه که عکس آنرا در پایین مشاهده می کنید دو گزینه وجود دارد:

در صورتی که شما گزینه Domain controller for a new domain را انتخاب کنید، یعنی اینکه می خواهید اولین DC را برای Domain خود ایجاد کنید.

و در صورتی که گزینه Additional domain controller for an existing domain را انتخاب نمایید، بدین معناست که شما از قبل یک DC، دارید و اکنون می خواهید یک DC جدید اضافه نموده و احتمالا آن را زیر شاخه ای از آن قرار دهید.

گزینه اول را انتخاب کرده و دکمه Next را کلیک نمایید.

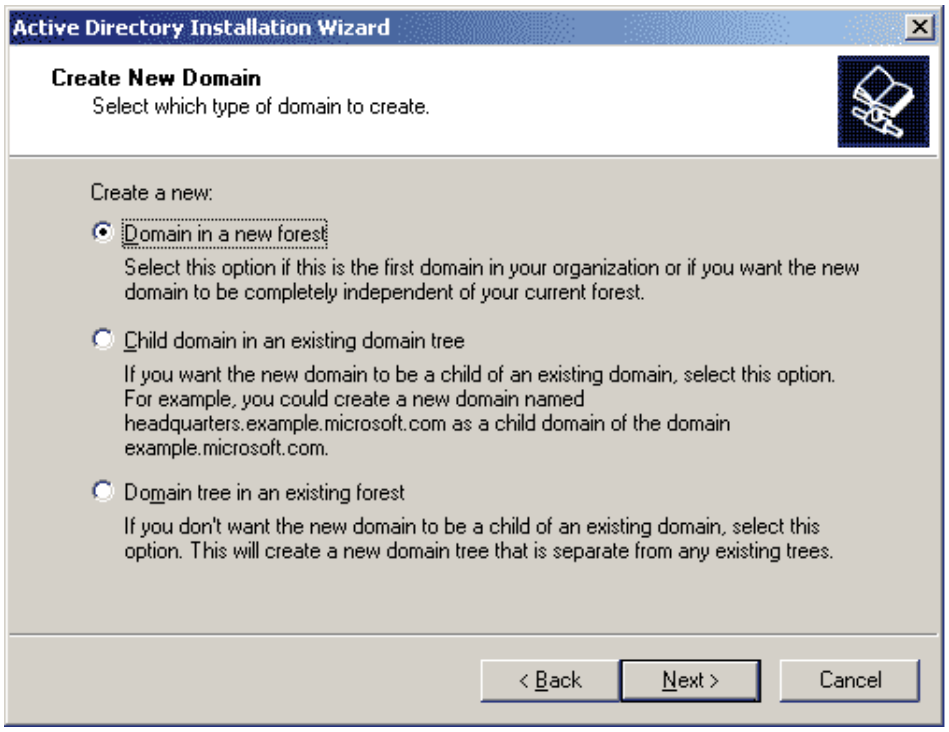


در صفحه بعدی با توجه به اینکه در صفحه قبل گزینه اول را انتخاب کرده اید، ۳ گزینه پیش رو دارید:

در صورتی که Domain ای که راه اندازی می کنید، اولین Domain برای یک Forest جدید می باشد، گزینه Domain in a new forest را انتخاب کنید. در این حالت یک Forest جدید ساخته خواهد شد. گزینه دوم (Child Domain in an existing domain tree) برای مواقعی می باشد که می خواهید یک Child Domain را در داخل یک Domain Tree که از قبل وجود داشته است، ایجاد کنید. و اما گزینه سوم (Domain tree in an existing forest) برای زمانی می باشد که شما نمی خواهید

Domain ای که ایجاد می شود به عنوان Child برای یک Domain Tree باشد و می خواهید این دامنه جدید به عنوان دامنه ریشه (نه فرزند دامنه ای دیگر) به کار گرفته شود.

گزینه اول را انتخاب کرده و بر روی Next کلیک کنید.



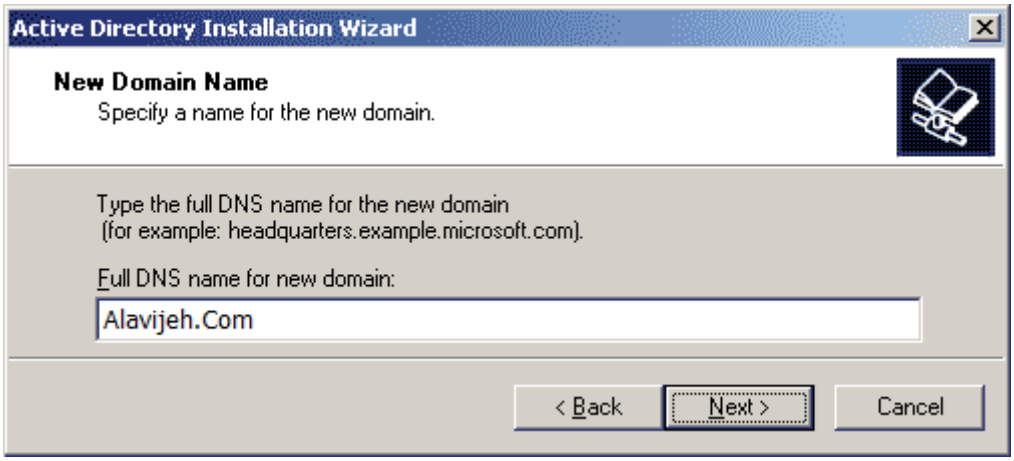
در اینجا مجددا توضیح مختصری درباره مفاهیم فوق می دهیم: ساختار Active Directory از یک مجموعه به نام Forest (جنگل) تشکیل می شود. هر Forest می تواند شامل یک یا تعدادی Domain Tree باشد. هر Domain Tree از یک یا چند Domain تشکیل می شود، به طوری که اولین Domain را با نام Root Domain و سایر Domainها را با نام Child Domain می شناسیم. هر Domain یک نام برای خود خواهد داشت که در سطح خود (نسبت به پدر) یکتا است و اسامی Domain های موجود در یک Tree به یکدیگر وابسته خواهند بود؛ یعنی نام فرزند با یک نقطه به ابتدای نام پدر خواهد چسبید. مثلاً اگر نام Domain پدر Alavijeh.Com و نام Domain فرزند Computer باشد، نام کامل فرزند (FQDN) می شود: Computer.Alavijeh.Com

در این صفحه که بسیار مهم می باشد شما می بایست نامی را که می خواهید برای Domain خود داشته باشید وارد نمایید. که بطور مثال بنده در این عکس Alavijeh.Com را در نظر گرفته ام. سپس روی دکمه Next کلیک کنید. دقایقی طول می کند تا سیستم تکراری بودن یا معتبر بودن نام وارد شده را بررسی کند.

برای انتخاب این اسم بایستی موارد زیر را در نظر داشته باشید:

۱. نام هیچ کامپیوتری در شبکه را برابر با نام Domain نگذارید.
۲. سعی کنید نامی را انتخاب کنید که بعدا زمانی که شبکه خود را به اینترنت وصل می کنید مشکل نداشته باشید. به عنوان مثال در صورتی که نام Domain خود را Microsoft.Com انتخاب کنید و شبکه خود را به اینترنت وصل کنید در داخل DNS یکسری مشکلات دارید و باید تنظیماتی را انجام دهید. (پیشنهاد می کنم که هر نامی را که دوست دارید انتخاب کنید و در انتهای آن .local را اضافه کنید چراکه پسوند .local در اینترنت وجود ندارد.)

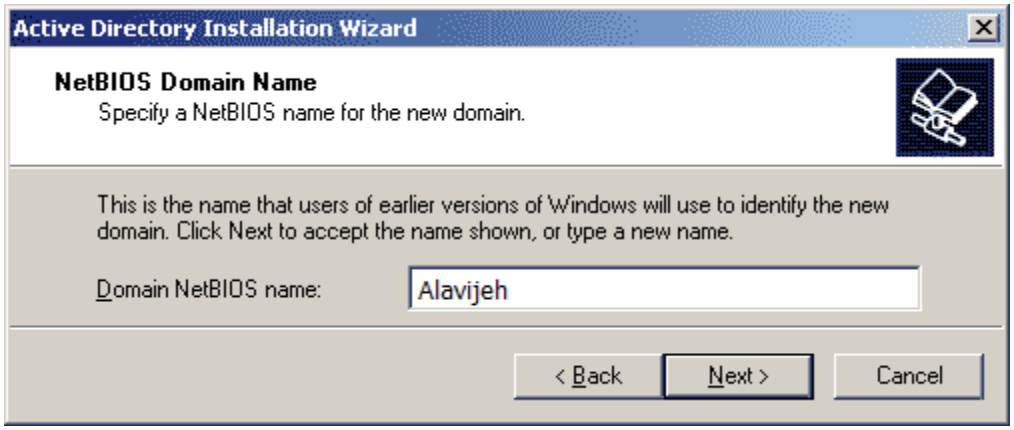
بعد از انتخاب نام و وارد کردن آن بر روی Next کلیک کنید تا وارد صفحه بعد شوید.



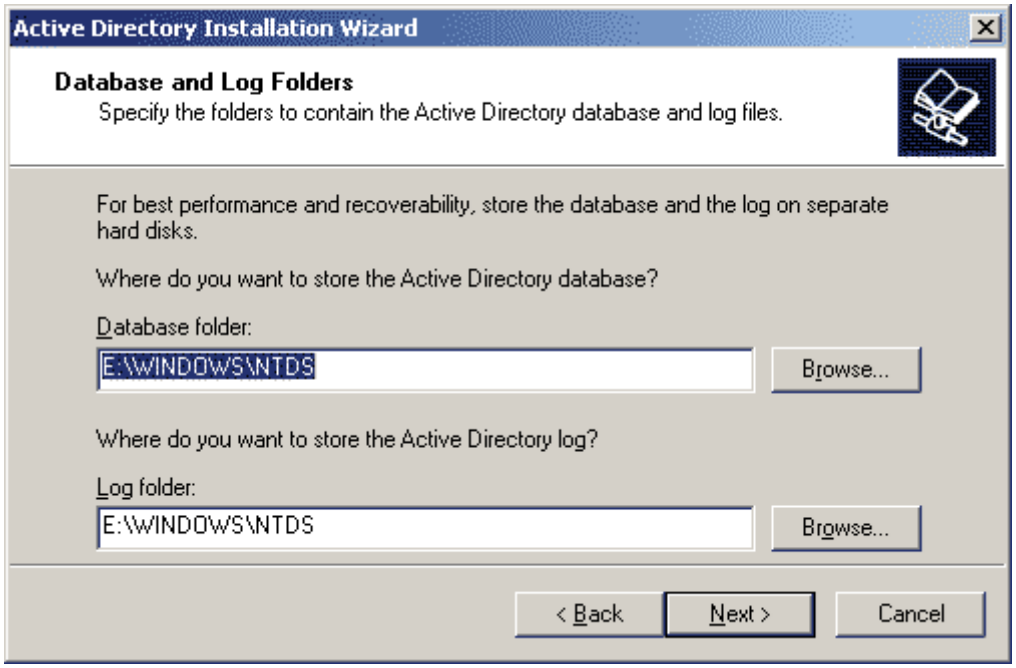
در صفحه بعدی نامی که وارد کردید تا قبل از نقطه به عنوان NetBIOS Name انتخاب می شود تا نسخه های قدیمی ویندوز از طریق آن Domain جدید را شناسایی کنند.

نکته در رابطه با NetBIOS Name: می دانیم که NetBIOS Name فرمت قدیمی نام گذاری مایکروسافت می باشد که این اسم از ۱۶ کاراکتر تشکیل می شود که ۱۵ تای ابتدایی آن را کاربر انتخاب می کند و آخرین کاراکتر را خود سیستم با توجه به سرویس های مختلف اضافه می کند.

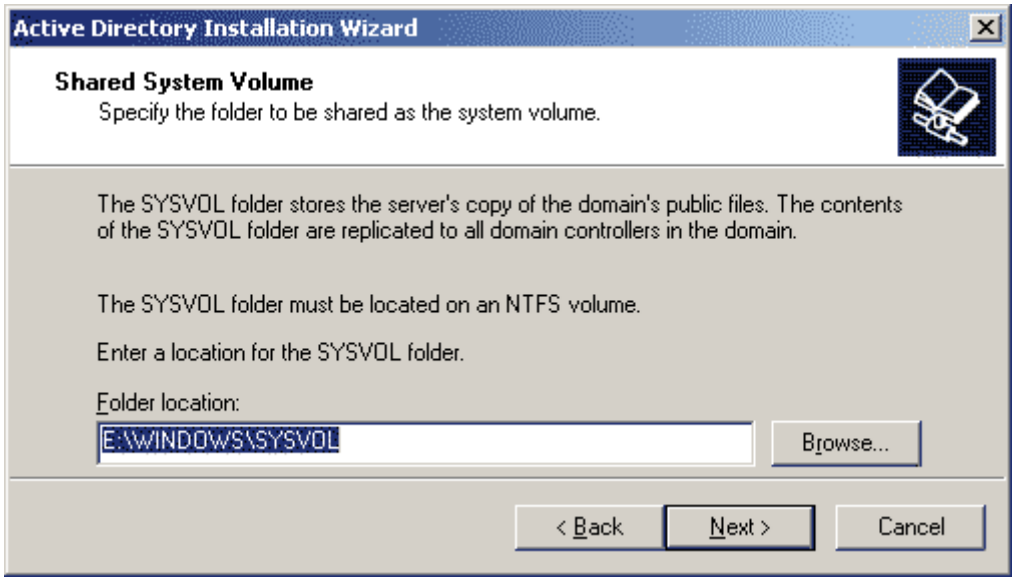
در این صفحه نیز بروی Next کلیک کنید.



در صفحه بعدی شما می توانید محل ذخیره Database، Active Directory و همچنین محل ذخیره Log فایل های مربوط به این سرویس را مشخص کنید.



قابل ذکر است که پایگاه داده اکتیو دایرکتوری به نام NTDS.DIT و به صورت پیش فرض در پوشه ویندوز ذخیره می شود. در صفحه بعدی شما محل ذخیره پوشه SYSVOL را مشخص می کنید.

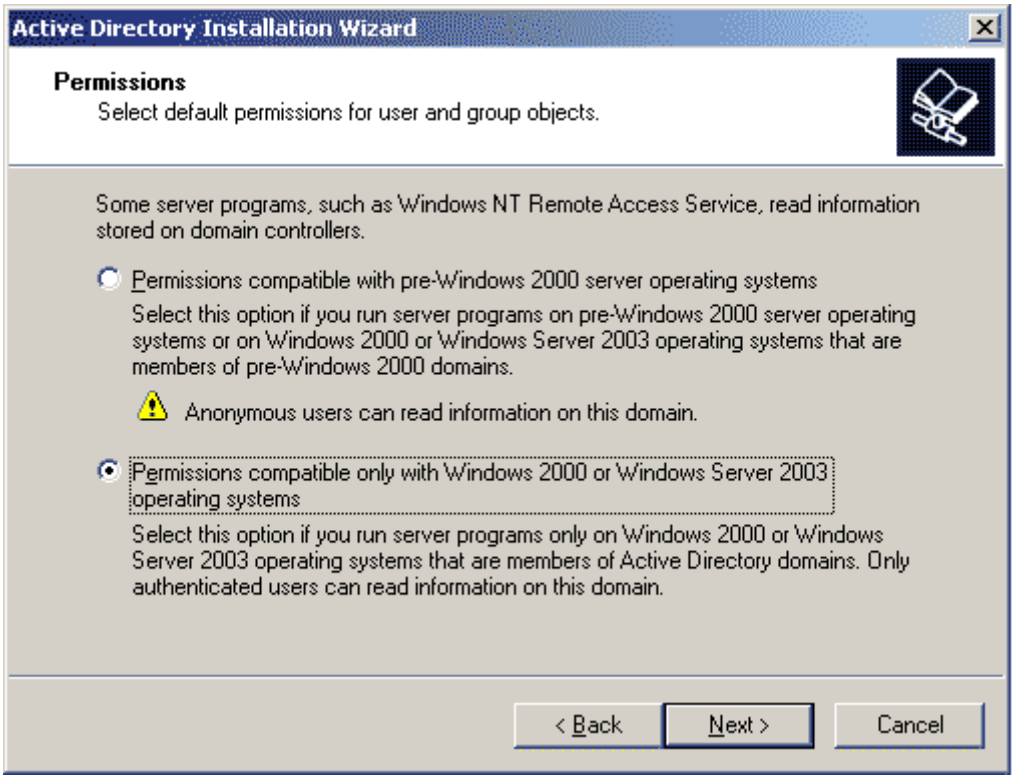


نکاتی در رابطه با پوشه SYSVOL:

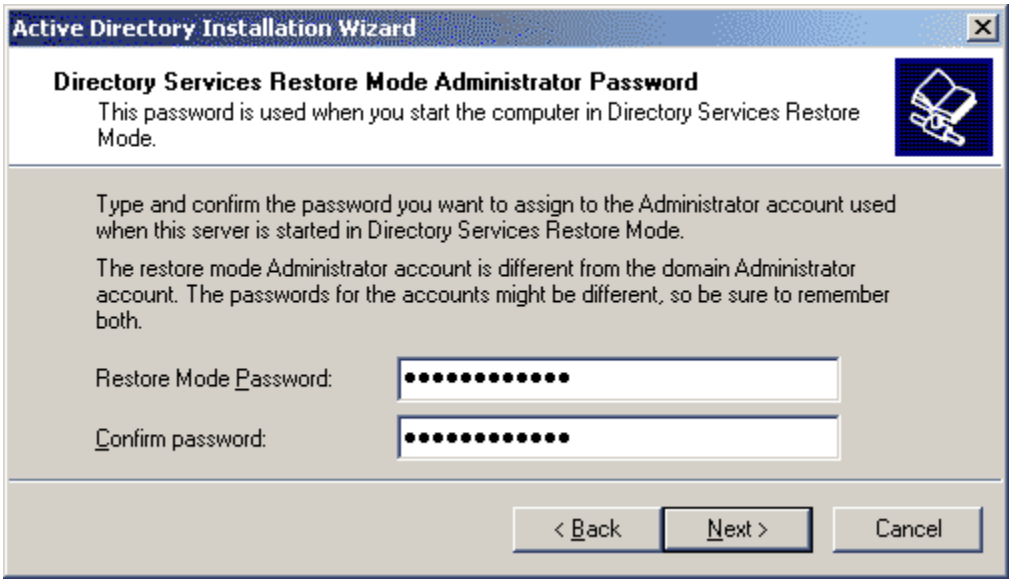
به هنگام نصب AD (اکتیو دایرکتوری) پوشه ای بر روی کامپیوتر DC ایجاد می شود که این پوشه به صورت پیش فرض Share شده می باشد. قابل ذکر است که محل این پوشه حتما باید بر پارتیشنی به فورمت NTFS باشد. فایلهای موجود در این پوشه حاوی سیاستهای کلی تعریف شده در داخل ساختار AD می باشد و همچنین DC ها برای اینکه بتوانند با یکدیگر عملیات Replication انجام دهند از این پوشه استفاده می کنند.

مر حله بعدی نصب DNS می باشد که می توانیم بگوییم که خود سیستم به صورت خودکار به همراه نصب AD، DNS هم نصب کند یا اینکه قبل از نصب AD سرویس DNS را خودمان به صورت دستی بر روی کامپیوتر مورد نظر نصب کنیم. و باید توجه داشته باشیم که وجود DNS برای AD الزامی است.

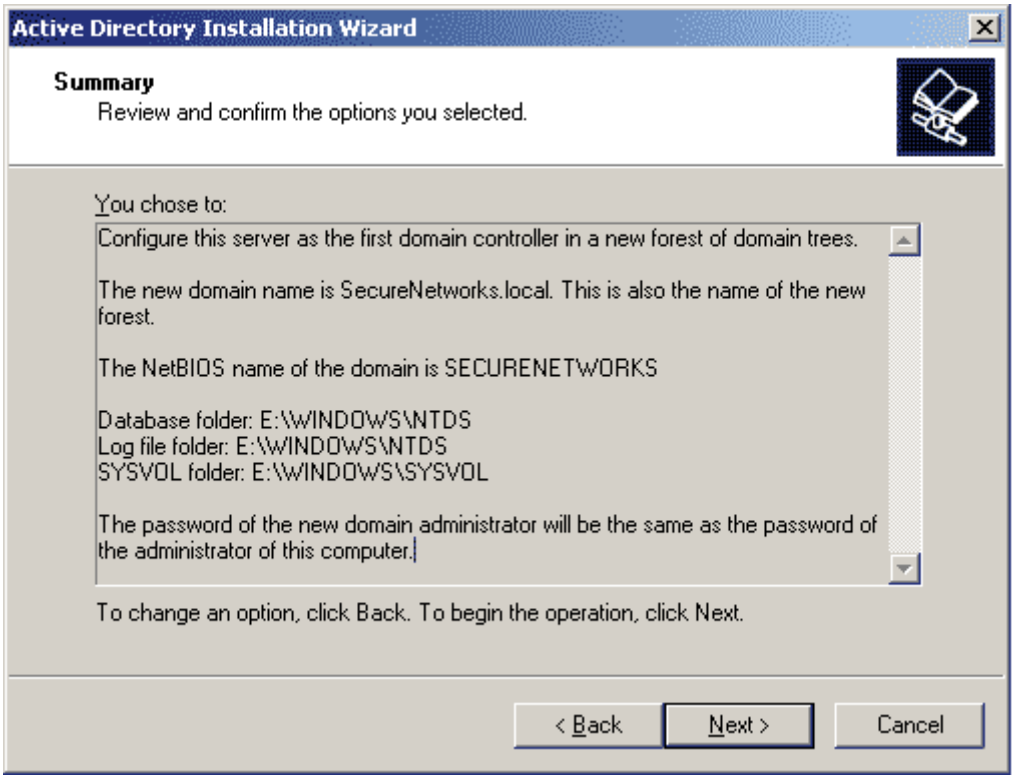
در مرحله بعدی انتخاب کلاینت هایی می باشد که با سرور ما ارتباط برقرار می کنند که گزینه اول برای پلاتفرم های قبل از ۲۰۰۰ می باشد و دومین گزینه پلاتفرم های ۲۰۰۰ و ۲۰۰۳ را پشتیبانی می کند که در شکل زیر مشاهده می کنید:



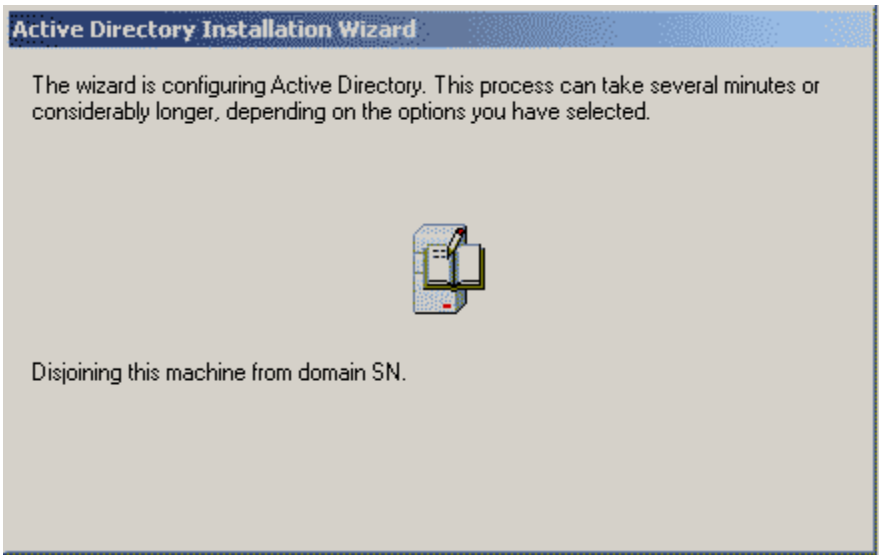
در صفحه بعدی که در شکل زیر مشاهده می کنید می بایست Password ای را برای حالت DSRM یا (Directory Services Restore Mode) انتخاب کنید تا در صورتی که کامپیوتر را در این حالت Boot کردید از این Password استفاده کنید.



و در صفحه نهایی تمامی تنظیماتی را که در صفحه های پیشین وارد نمودید به طور یکجا و به صورت Information نشان می دهد. در صورتی که مشکلی نمی بینید و تمامی تنظیمات درست است بر روی Next کلیک کنید تا عملیات نصب آغاز شود.



پس از Next کردن صفحه زیر برای شما نمایان خواهد شد که عملیات مختلف راه اندازی DC و نصب AD را نشان می دهد:



پس از پایان یافتن عملیات نصب بر روی Finish کلیک نمایید و با پیغامی که ظاهر می شود دستگاه خود را Restart کنید تا تمام عملیات انجام شده بر روی سیستم شما اعمال شود.

اجازه می دهیم سیستم مجدد راه اندازی شود.

پس از طی مراحل فوق شما موفق به نصب قویترین سرویس مایکروسافت بر روی ویندوز سرور خود شده اید.

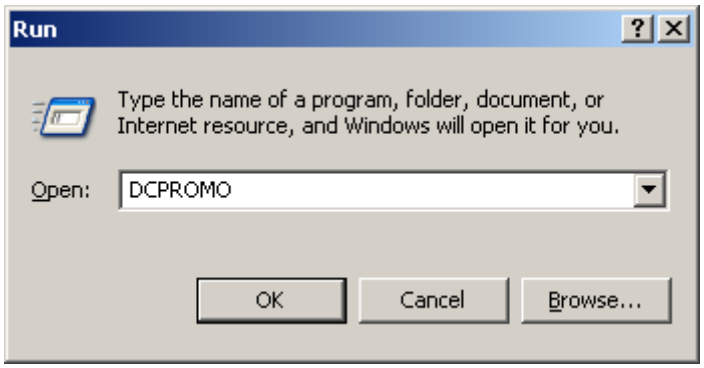
پس از راه اندازی سیستم میتوانیم با استفاده از کلمه کاربری مدیر سیستم (Administrator) و کلمه رمزی که در هنگام نصب وارد کرده ایم وارد سیستم شویم.

در هنگامیکه این سرویس بر روی ویندوز سرور نصب می گردد کلیه Account ها، Group های ویندوز غیرفعال شده و جای خود را به گروهها و User های Active Directory می دهند.

حال کافیست پیکربندی آن را انجام دهید.

۲-۱۹- حذف Active Directory

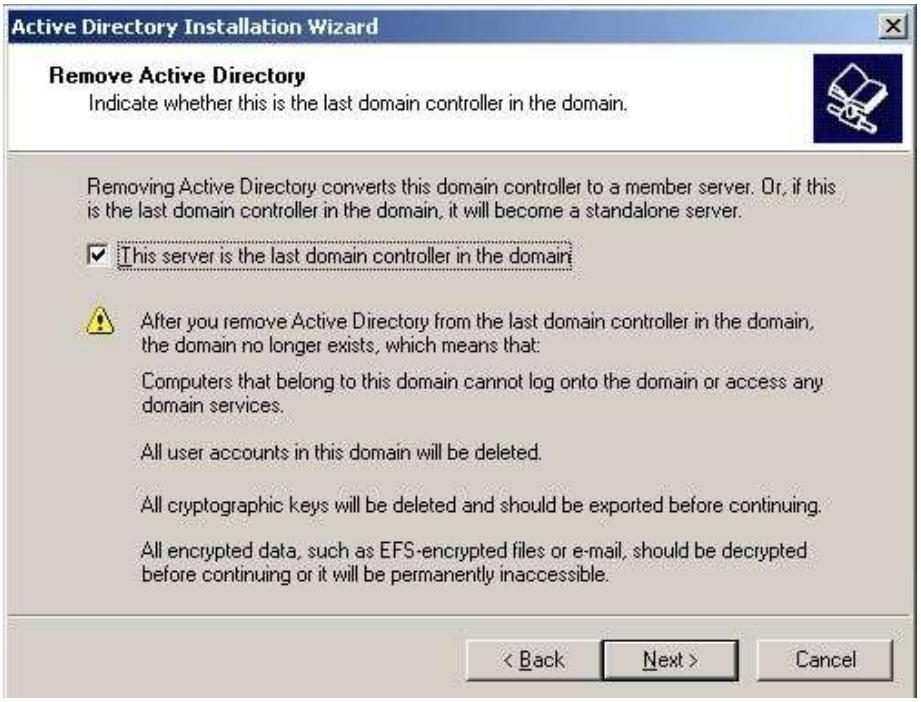
حذف Active Directory بسیار شبیه نصب آن است. همانطور که برای نصب Active Directory از دستور DCPromo استفاده کردیم، برای حذف نیز همین دستور را در Run وارد می کنیم:



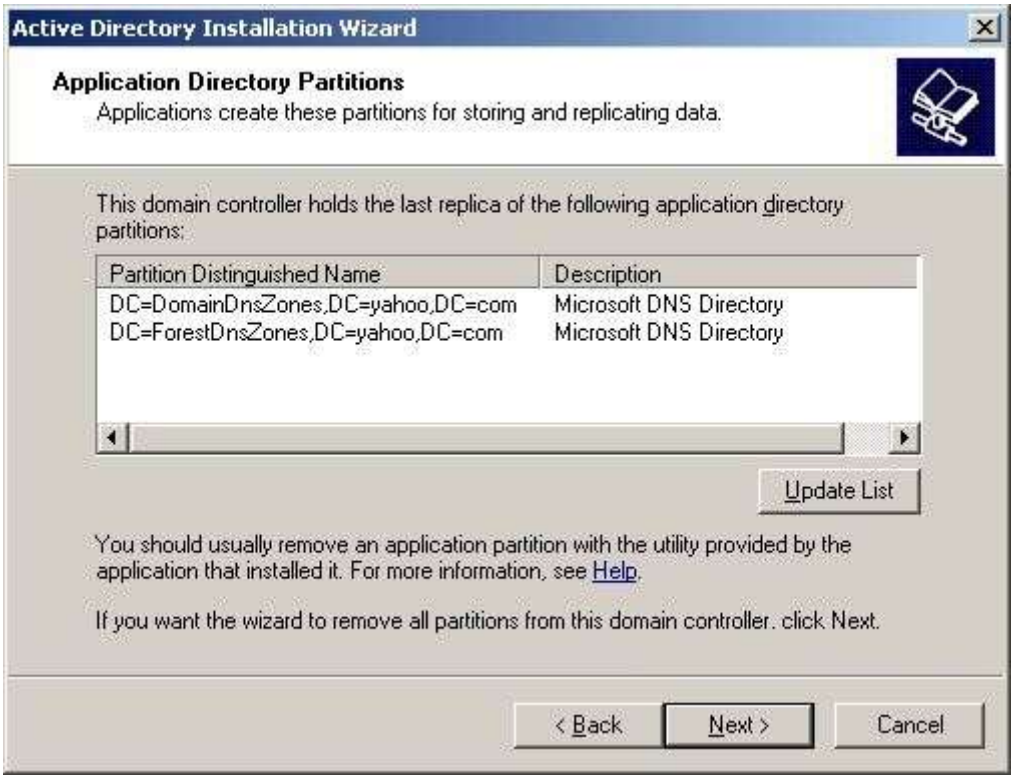
پس از کلیک کردن روی دکمه OK، صفحه خوش آمد گویی می شود. بر روی دکمه Next کلیک کنید.

سپس پیغام زیر ظاهر می شود. روی دکمه OK کلیک کنید:

در این صفحه بایستی مشخص کنید که این کامپیوتر یک کنترل کننده دامنه (DC) می باشد. با حذف DC، این کامپیوتر تبدیل به یک کامپیوتر عادی عضو شبکه می شود. برای ادامه عملیات حذف، روی دکمه Next کلیک کنید:



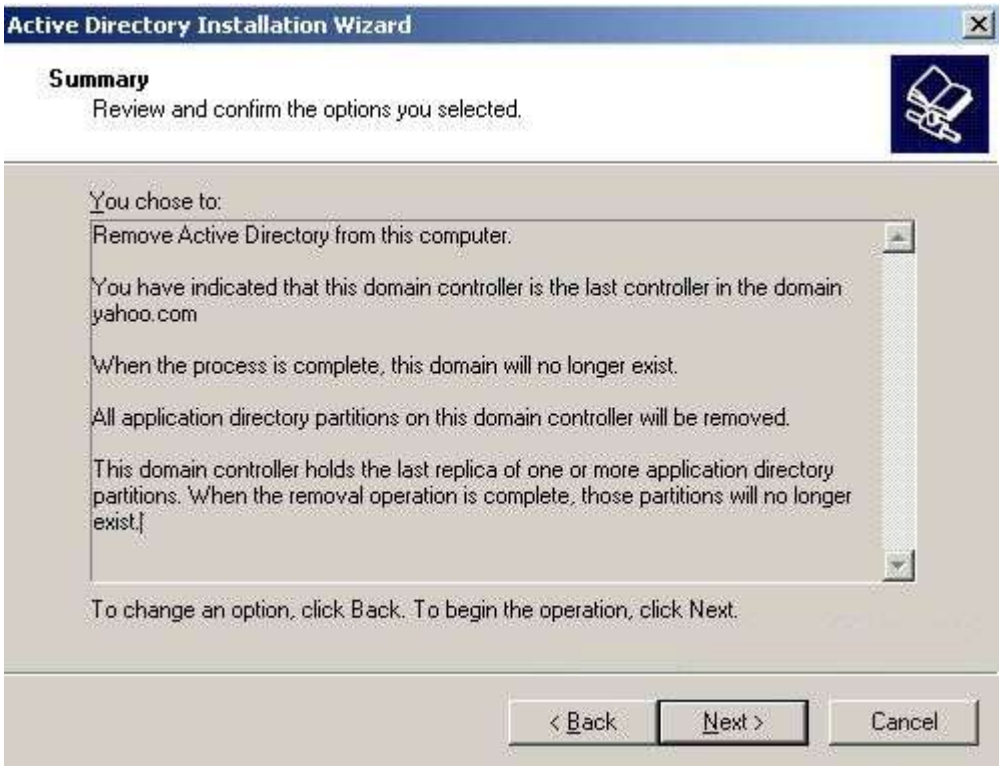
مجددا روی دکمه Next کلیک کنید:



سپس در این صفحه بایستی مشخص نمایید که قصد دارید دایرکتوری برنامه های کاربردی اکتیو دایرکتوری را حذف نمایید. عمل حذف دایرکتوری برنامه های کاربردی اکتیو دایرکتوری بعد از پایان پذیرفتن عملیات حذف اکتیو دایرکتوری رخ می دهد.

باز هم روی دکمه Next کلیک کنید. در این پنجره از کاربر کلمه رمزی را برای کاربر مدیر کامپیوتر درخواست می شود که بعد از حذف این سرویس و راه اندازی مجدد سیستم، کاربر می بایستی توسط این کلمه عبور وارد سیستم گردد.

سپس روی دکمه Next کلیک کنید:



بعد از رفتن به مرحله بعد، سیستم شروع به حذف Active Directory خواهد کرد. در این قسمت بایستی چند دقیقه ای صبر کنیم تا سیستم کارش به اتمام برسد.

پس از اتمام حذف Active Directory، روی دکمه Finish کلیک کنید.

در نهایت سیستم را Restart کنید:

۱۹-۳- مفاهیم Active Directory Backup

امروزه تهیه پشتیبان از فایل ها، اسناد و داده ها در هر شبکه و سیستمی، خواه شبکه کوچک باشد یا بزرگ، ضروری به نظر می رسد؛ حتی تهیه پشتیبان بر روی رایانه های شخصی هم گاهی واجب می باشد. در همین راستا پشتیبان گیری از Active

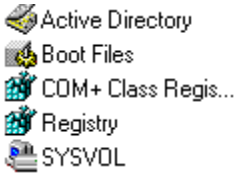
Directory هم در جهت نگهداری و پشتیبانی از آن یکی از اصول پایه و مهم به شمار می آید؛ زیـرا Active Directory قلـب یک شبکه Client/Server به حساب می آید.

تهیه پشتیبان از Active Directory را به ۲ صورت گرافیکی و توسط خط فرمان می توان انجام داد که در این آموزش هـر دو صورت بررسی خواهد شد.

پشتیبان گیری مرتب و طبق زمانبندی مناسب سبب می شـود تـا در مواقـع بحرانـی از دسـت دادن داده و اطلاعـات شـانس بیشتری در جهت برگرداندن آنها داشته باشید.

برای تهیه پشتیبان از Active Directory مـی بایسـت از System State پشـتیبان تهیـه کنیـد، پشـتیبان گیـری از Active Directory هیچ گونه خللی در کار Domain Controller و شبکه ایجاد نمی کند.

System State دارای اجزای مختلفی می باشد، که این اجزا بر روی سیستمی که نقـش Domain Controller ایفـا مـی کنـد متفاوت از دیگر سیستم ها می باشد. در این جا، اجزای تشکیل دهنده آن در یک کنترل کننده دامنه را مورد بررسی قرار مـی دهیم:



۱. Active Directory
۲. Boot Files
۳. COM+ Class Registration Database
۴. Registry
۵. SYSVOL
۶. Certificate Service Database

نکته:

موارد ۱ و ۵ فقط بر روی Domain Controller وجود دارند که جزیی از System State هستند.

مورد ۶ فقط بر روی سیستمی که CA سرور باشد وجود خواهد داشت.

اکثر اجزای در بالا ذکر شده را می توان از طریق نامشان به کاربردشان پی برد و فقط به توضیحی کوتـاه در مـورد SYSVOL می پردازیم:

SYSVOL یک پوشه به اشتراک گذاشته شده می باشد که حاوی قالب های Group Policy و اسکریپتهای Logon می باشد.

هر چند System State دربر دارنده اکثر تنظیمات سیستم می باشد، ولی الزاما حاوی تمام فایل ها و اطلاعات مورد نیاز بـرای برگرداندن کامل سیستم به قبل از خرابی و مشـکل نمـی باشـد. البتـه بـرای برگردانـدن اطلاعـات Active Directory تهیـه پشتیبان از آن کافی است؛ برای تهیه پشتیبان کامل از سیستم می توان از ابزارهایی نظیر Norton Ghost بهره جست.

نکته مهم: در هنگام تهیه پشتیبان از Active Directory باید به زمان مشخص شده برای Tombstone (سـنگ قبـر) توجـه داشته باشیم، از آن رو که نمی توان آن پشتیبان گرفته شده را بعد از مدت زمان مشخص شده برای Tombstone باز گردانـد. زمان پیش فرض ۶۰ روز می باشد که اگر ویندوز بروز رسانی شده باشد تا ۱۸۰ روز هم قابل افزایش می باشد. پس سعی کنید در بازه های زمانی کوتاه پشتیبان گیری صورت گیرد و حداقل ۲ پشتیبان در زمان Tombstone داشته باشید.

Tombstone چیست؟

وقتی یک Object را از Active Directory پاک می کنیم در مرحله اول بطور فیزیکی از پایگاه داده حـذف نمـی شـود؛ بلکـه Active Directory مشخصه isDeleted (attribute) را True کرده و آن را به یـک Container خـاص بـه نـام CN=Deleted انتقال می دهد، حالا این Object یک Tombstone می باشد که با استفاده از ابزارهای معمول قابل مشاهده نمی باشد.

می توان با استفاده از این خاصیت، Objectهایی که اشتباها پاک شده اند را حتی بدون استفاده از Backup&Restore بازیابی کرد. یکی از ابزارهایی که می تواند Tombstoneها را باز گرداند، AdRestore می باشد.

شرکت مایکروسافت داشتن حداقل ۲ سرور Domain Controller را توصیه کرده است، چنانکه در صورت خرابی سرور اصلی، سرور پشتیبان وظایف آن را به عهده می گیرد و خللی در کار شبکه به وجود نمی آید؛ البته فقط یک سرور می تواند در بر دارنده Operations Master Role ها باشد و در صورت از دست دادن کامل DC اصلی این ها را به DC دیگر انتقال می دهیم.

DC های پشتیبان را Additional Domain Controller می نامند و هنگام نصب Active Directory در پنجره Active Directory Type باید Additional Domain Controller for existing Domain را انتخاب کرد.

هر چند داشتن Additional Domain Controller ریسک از دست دادن اطلاعات را کاهش می دهد، ولی برای باز گردانی اطلاعات به صورت Authoritative (در ادامه بررسی می شود) به کپی پشتیبان System State نیاز خواهید داشت.

ایجاد تغییراتی برای آزمایش:

برای اینکه پشتیبان گیری و بازگرداندن آن قایل لمس باشد، یک کاربر با نام Reza ایجاد کنید.

۱۹-۴- پشتیبان گیری از Active Directory

همان طور که اشاره شد برای پشتیبان گیری از Active Directory باید از System State پشتیبان تهیه کنیم، برای این منظور کاربری که قصد گرفتن پشتیبان دارد باید عضو گروه Domain Admins باشد تا بتواند این عملیات را انجام دهد.

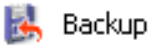
توجه داشته باشید که برای تهیه پشتیبان باید حتما به صورت Local از ابزار Backup Utility استفاده کنید زیرا پشتیبان System State را نمی توان از راه دور تهیه کرد، البته می توان از Remote Desktop جهت اجرای این ابزار به صورت Local بهره جست.

۱۹-۴-۱- پشتیبان گیری توسط رابط گرافیکی

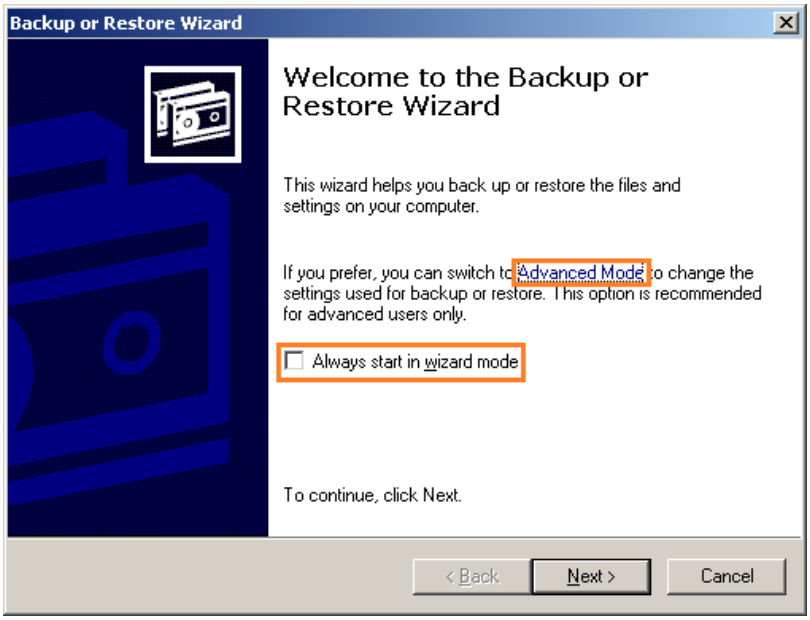
برای تهیه پشتیبان مراحل زیر را طی می کنیم:

۱. از منوی شروع آدرس زیر را جهت اجرای Backup Utility طی می کنیم:

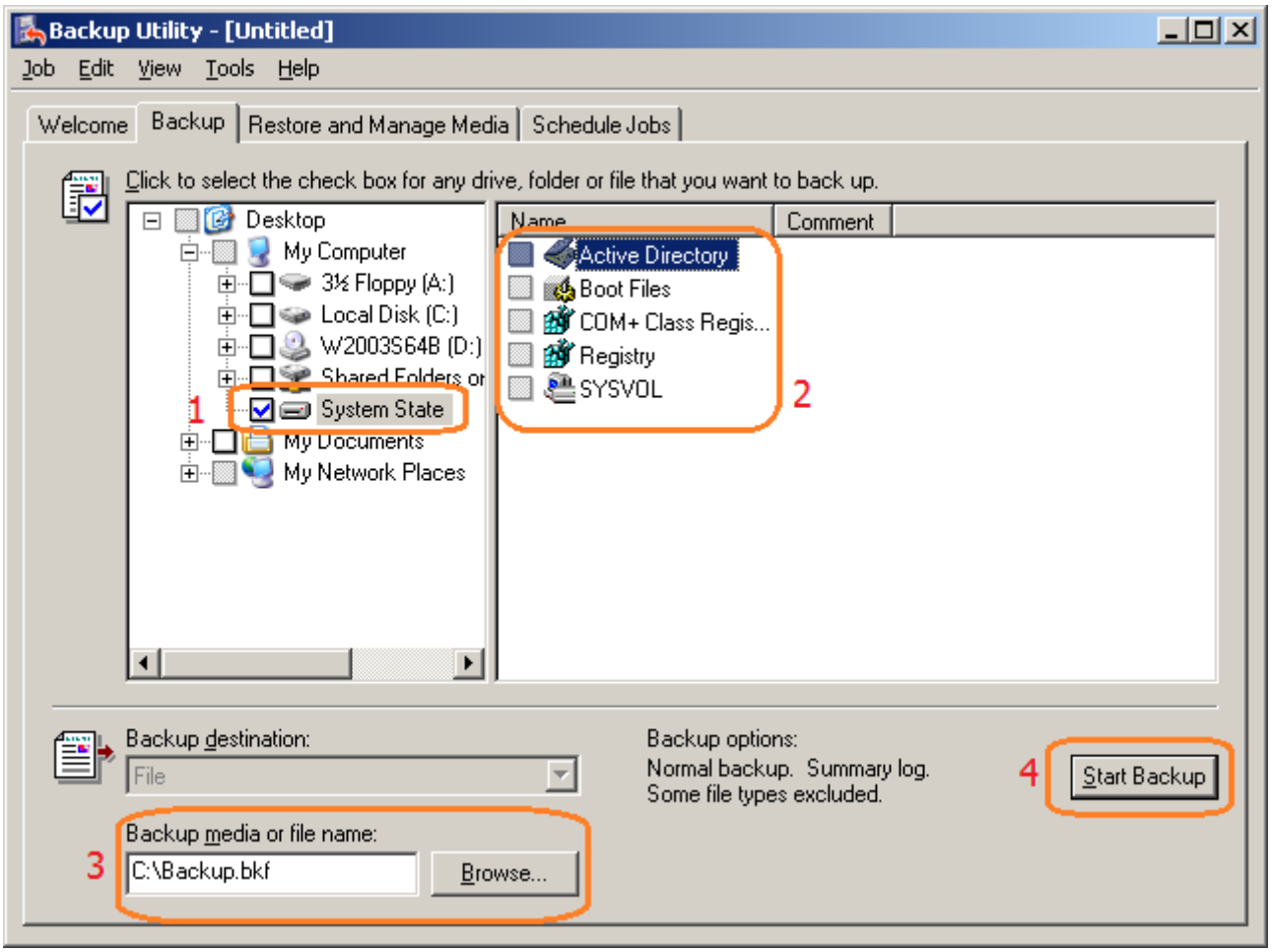
Start Menu ➔ All Programs ➔ Accessories ➔ System Tools ➔ Backup



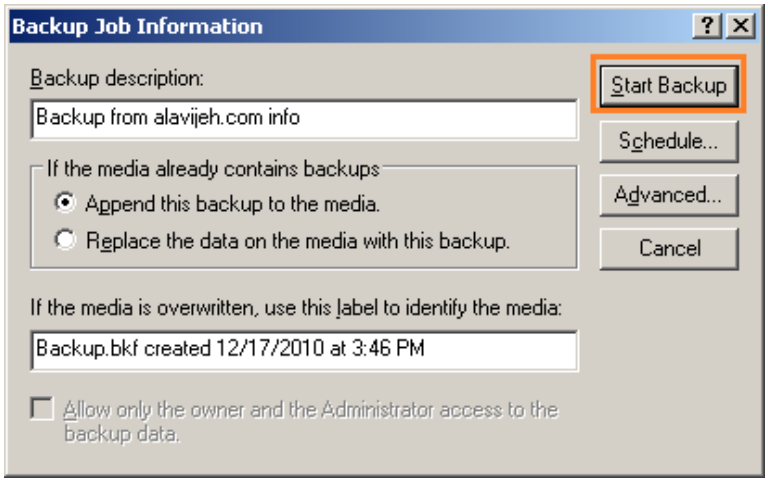
۲. در پنجره Backup or Restore Wizard طبق عکس زیر بر روی Advance mode کلیک کنید. اگر می خواهید همیشه در حالت پیشرفته اجرا شود، تیک Always start in wizard mode را بردارید.



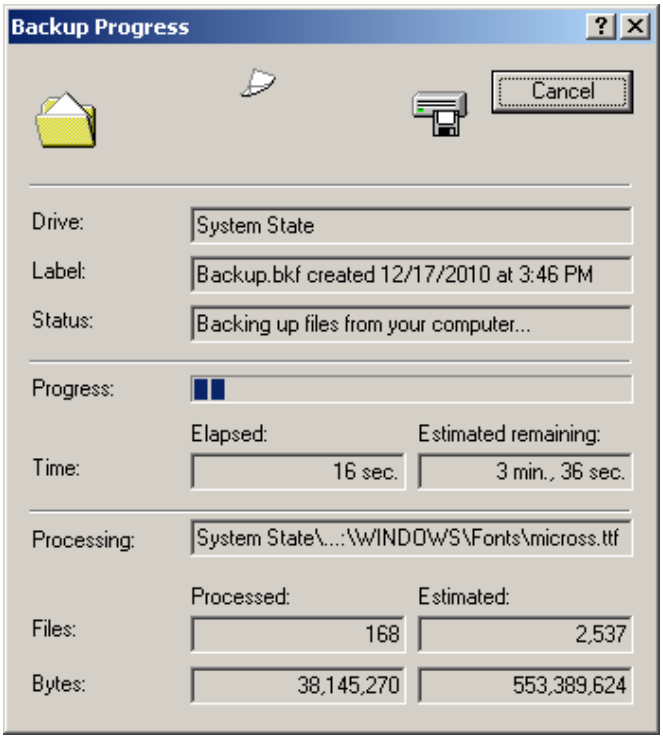
۳. وارد سربرگ Backup شده و طبق عکس زیر، System State را انتخاب و تیک آن را بزنید. سپس از دکمه Browse محلی که می خواهید پشتیبان در آنجا ذخیره شود را مشخص و نامی مناسب برای آن انتخاب کنید، سپس بر روی Start Backup کلیک کنید.



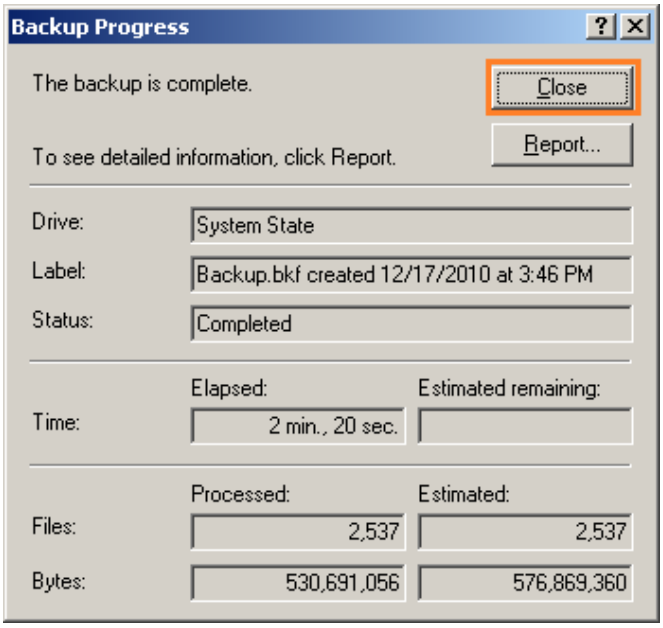
۴. در پنجره Backup Job Information بر روی Start Backup کلیک کنید. همچنین می توانید برای یک پشتیبان گیری مرتب در همین مرحله بر روی Schedule کلیک کنید و زمانبندی مناسب را انجام دهید.



۵. با کلیک روی Start Backup، عملیات کپی گیری شروع می شود. صبر کنید تا این عمل تمام شود.



۶. در این مرحله پشتیبان گیری شروع و پایان می پذیرد، در آخر بر روی Close کلیک کنید.

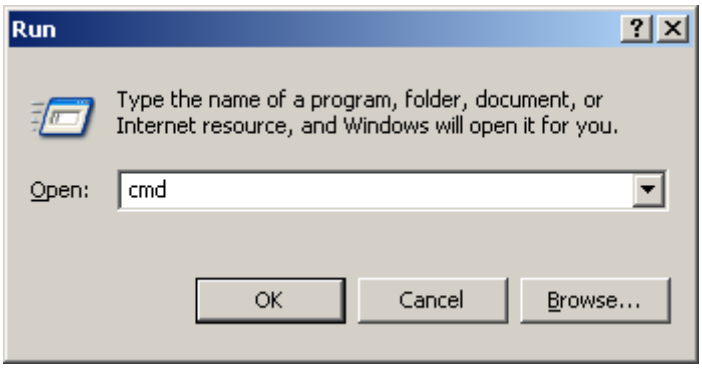


توجه: توصیه می شود پشتیبان را حتما در حالت Normal انجام دهید و از انواع دیگر پشتیبان گیری مانند Incremental یا Differential خودداری کنید.

۱۹-۴-۲- پشتیبان گیری توسط خط فرمان

برای تهیه پشتیبان توسط خط فرمان (Command Line) مراحل زیر را طی کنید:

۱. از منوی Start برنامه CMD را از آدرس زیر اجرا کنید.



۲. در خط فرمان با استفاده از دستور ntbackup به صورت زیر می توان پشتیبان تهیه کرد:

Ntbackup backup systemstate /J 'Backup Job' /F 'C:/systemstate.bak'

ntbackup: ابزار پشتیبان گیری از طریق خط فرمان می باشد.

Backup: مشخص کننده این است که عملیات پشتیبان گیری صورت می پذیرد.

Systemstate: مشخص کننده این است که از System State پشتیبان گرفته می شود.

F/: نام فایل پشتیبان و محل آن را مشخص می کند.

ایجاد تغییراتی برای آزمایش:

اکنون برای آزمایش باز گردانی اطلاعات کاربر Reza که ایجاد کرده بودید را حذف کنید.

۱۹-۵- بازگرداندن اطلاعات Restore Active Directory

در ویندوز سرور ۲۰۰۳ برای باز گردانی پایگاه داده Active Directory در صورت تنظیمات اشتباه، خرابی یا از دست دادن اطلاعات، به دلیل مشکلات سخت افزاری و نرم افزاری شیوه های مختلفی وجود دارد. در ساده ترین حالت در صورت وجود چندین DC می توان DC دیگری را نصب و سپس به واسطه Replication بین DC ها تمامی اطلاعات به DC جدید منتقل خواهد شد؛ راه دیگر استفاده از ابزار پشتیبان گیری برای بازگرداندن اطلاعات می باشد.

توجه داشته باشید که وقتی از یک Domain Controller پشتیبان تهیه می کنید، از تمامی داده های Active Directory به همراه پوشه SYSVOL و Registry بر روی سرور پشتیبان گرفته می شود. پس در موقع بازگرداندن آن، هر آنچه پشتیبان گرفته شده همچون تنظیمات Group Policy و رجیستری هم به حالت قبل باز می گردد.

۱۹-۵-۱- شیوه های بازگرداندن پشتیبان

برای بازگرداندن پشتیبان Active Directory، 3 روش وجود دارد:

۱. **Primary**
۲. **Normal (NonAuthoritative)**
۳. **Authoritative**

۱. **Primary**: این شیوه اولین Domain Controller را مجددا ایجاد می کند، وقتی هیچ راه دیگری برای ایجاد دوباره Domain وجود ندارد. این شیوه زمانی کاربرد دارد که هیچ DC دیگری در شبکه وجود ندارد و می خواهید DC اصلی را توسط پشتیبان مجدد ایجاد کنید.

۲. **Normal**: این شیوه دوباره Active Directory را به حالت قبل از پشتیبان گیری بر می گرداند و سپس به واسطه Replicate بین DC ها بروز می شود. این شیوه زمانی استفاده می شود که چندین DC در شبکه وجود دارد و می خواهید یک DC را به آخرین وضعیت مناسب آن بر گردانید.

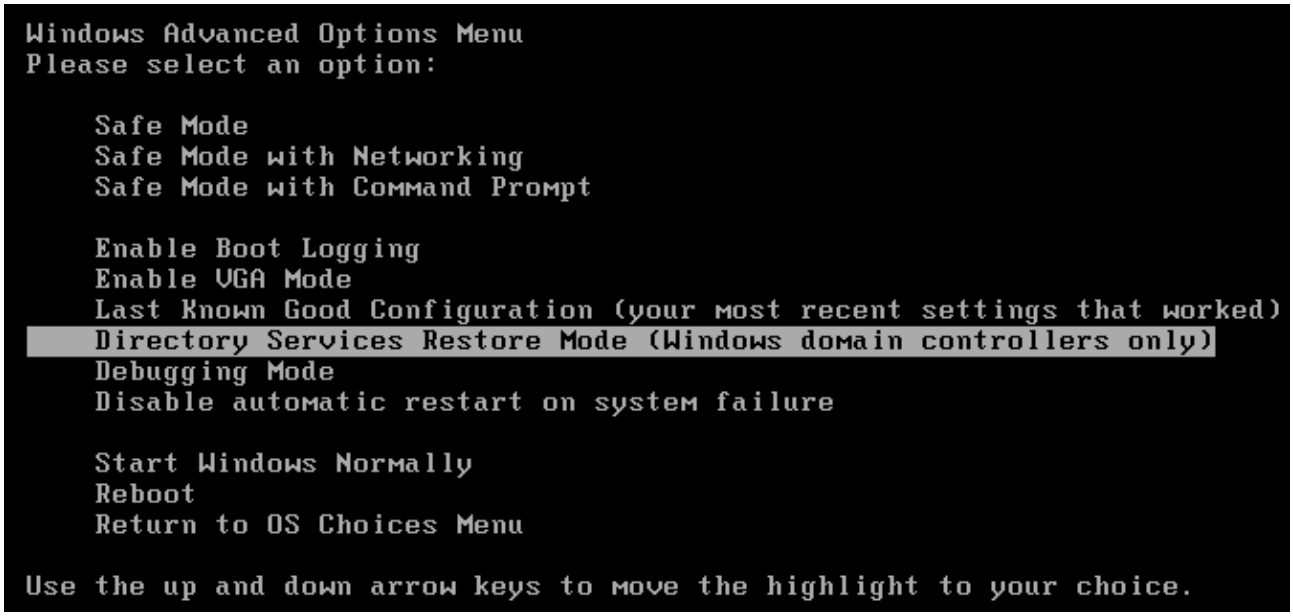
۳. **Authoritative**: این شیوه پشت سر Normal استفاده می شود. بدین معنی که مراحل همانند Normal صورت می پذیرد؛ منتها در آخر کار، یک سری داده ای مشخص را نشانه دار می کنید تا در Replicate بین DC ها برعکس Normal بازنویسی نشوند.

فرض کنید اشتباها یک OU را حذف کرده اید و در Replicate بین دومین ها این OU در تمام DC های دیگر هم حذف شده است، هم اکنون برای باز گرداندن آن فقط می توانید از شیوه Authoritative استفاده کنید، زیرا به علت وجود DC از شیوه Primary نمی توان استفاده کرد، در صورت استفاده از Primary کلیه اطلاعات بعد از پشتیبان گیری از بین می رود؛ در صورت استفاده از شیوه Normal به خاطر Replicate بین DC ها، OU که در DC های دیگر پاک شده است در DC جدید هم پاک می شود پس باید با مشخص کردن آن به صورت Authoritative از بازنویسی آن جلوگیری کرد.

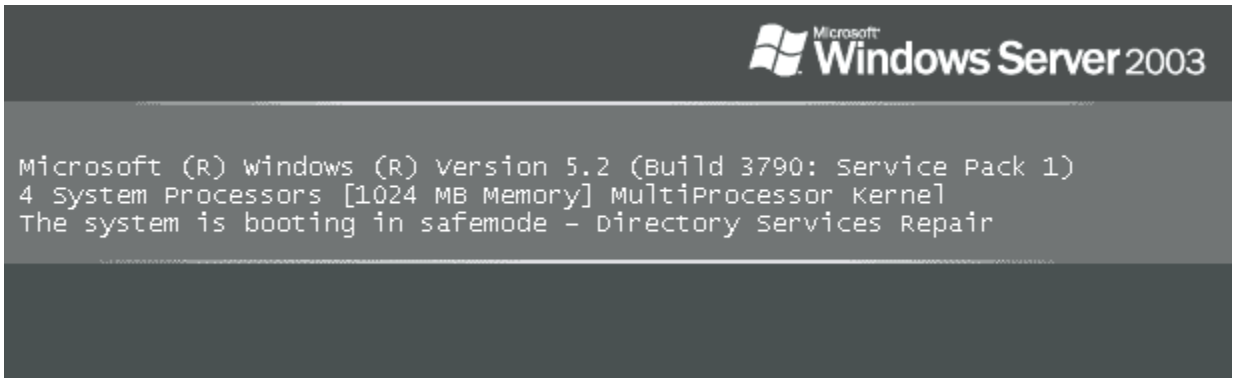
۱۹-۵-۲- نحوه بازگرداندن به صورت Primary

برای بازگرداندن پشتیبان مراحل زیر را طی کنید:

۱. Domain Controller (کامپیوتر سرور) را در حالت Directory Services Restore Mode شروع مجدد کنید. یعنی قبلاً از بالا آمدن ویندوز، کلید F8 را فشار دهید تا صفحه زیر نمایان شود. در این صفحه گزینه Directory Services Restore Mode را انتخاب نمایید.



۲. بدین ترتیب سیستم در حالت Safe Mode و AD Repair بالا می آید.

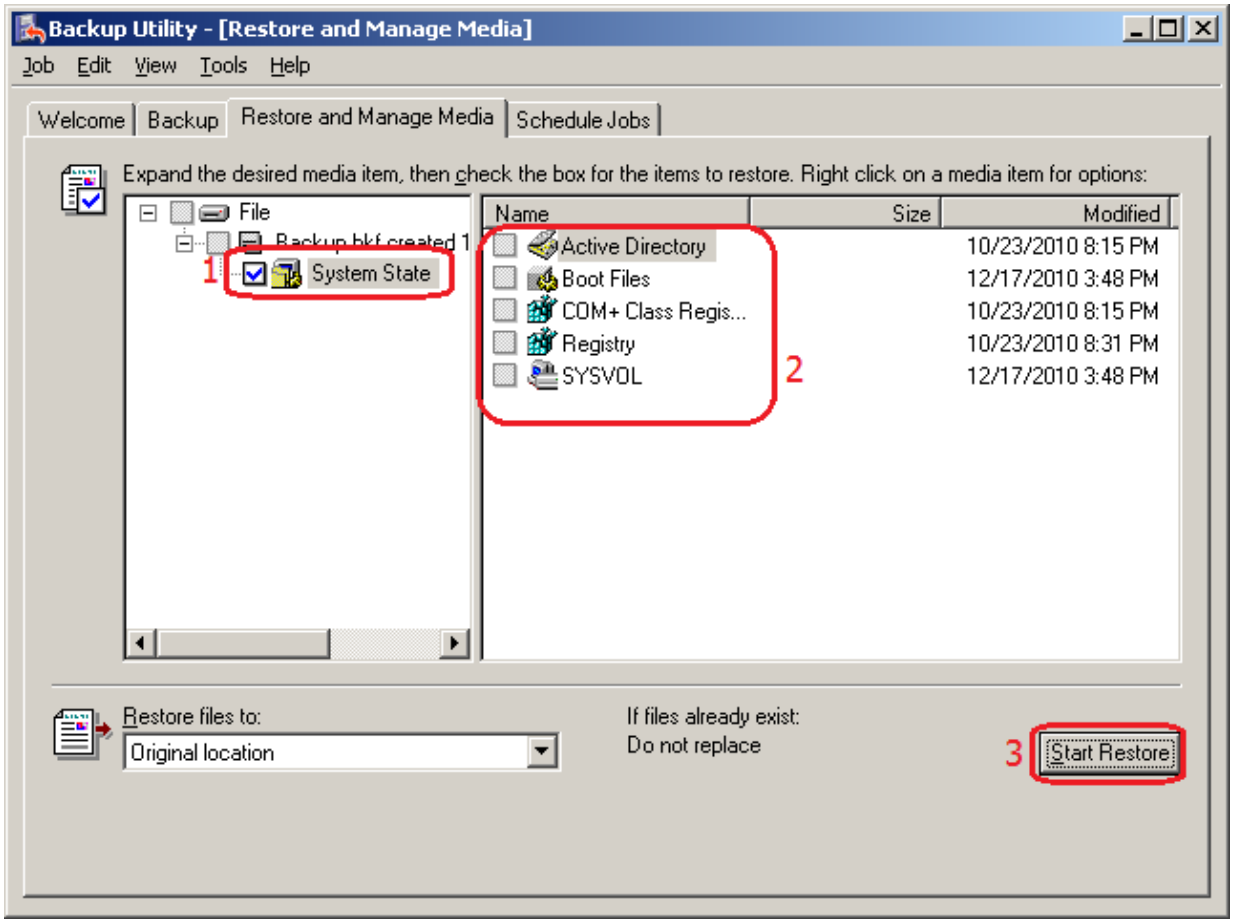


۳. از منوی شروع آدرس زیر را جهت اجرای Backup Utility طی می کنیم:

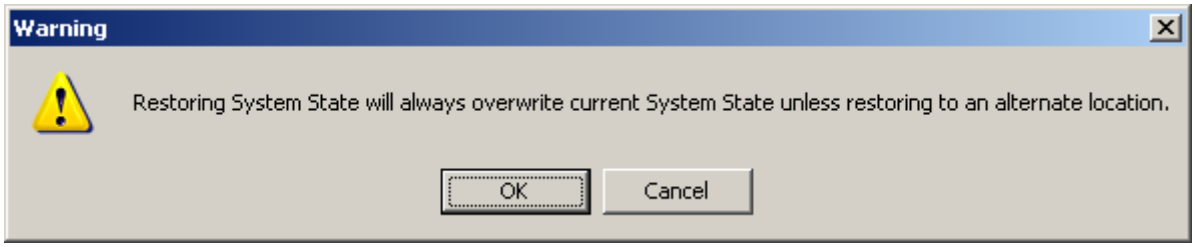
Start Menu ➔ All Programs ➔ Accessories ➔ System Tools ➔ Backup

Backup

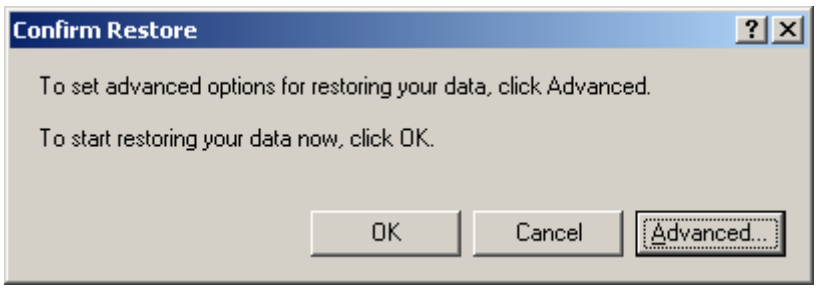
۴. در پنجره Backup or Restore Wizard بر روی Advance mode کلیک کنید. (به تصاویر بالایی مراجعه نمایید). در سربرگ Restore and Manage Media هر آنچه که می خواهید بازگردانید (که در اینجا System State می باشد) را انتخاب و سپس بر روی Start Restore کلیک کنید.



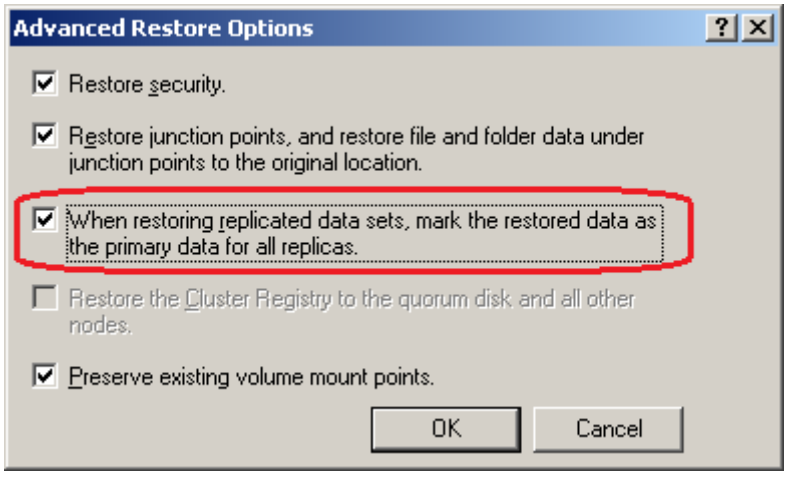
۵. یک صفحه هشدار دهنده باز می شود که OK را می بایست انتخاب کنید.



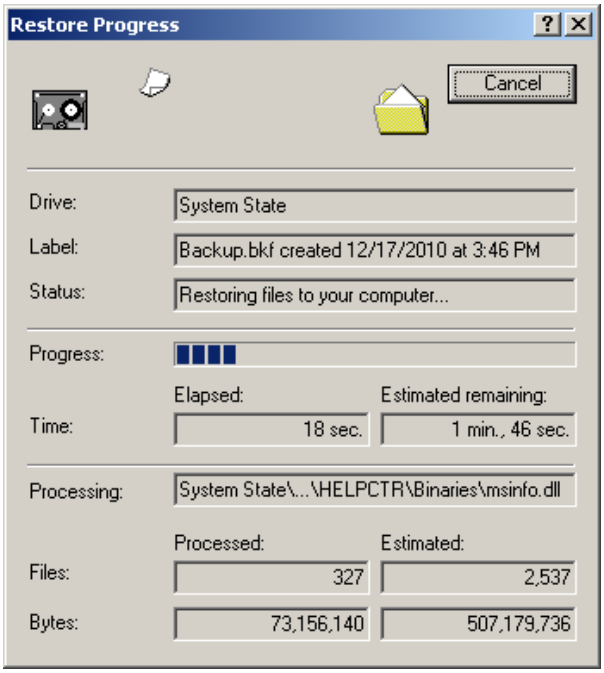
۶. در Confirm Restore بر روی Advanced کلیک کنید.



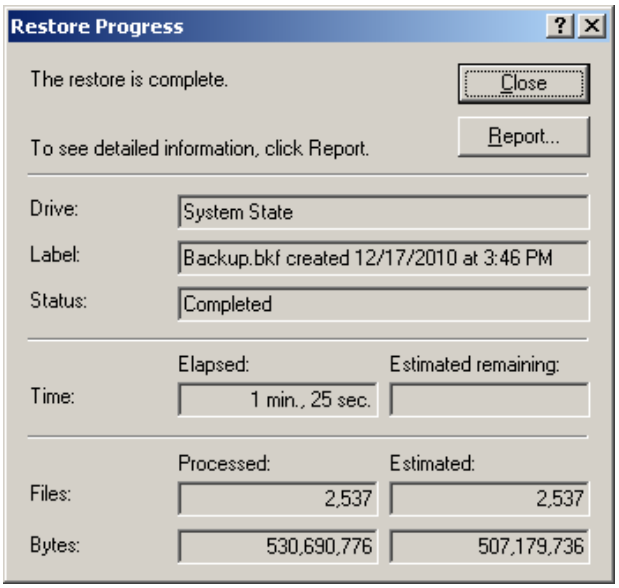
۷. در پنجـره Advanced Restore options، گزینـه When restoring replicated data sets, mark the restored data as the primary data for all replicas را انتخاب و سپس بر روی OK کلیک کنید.



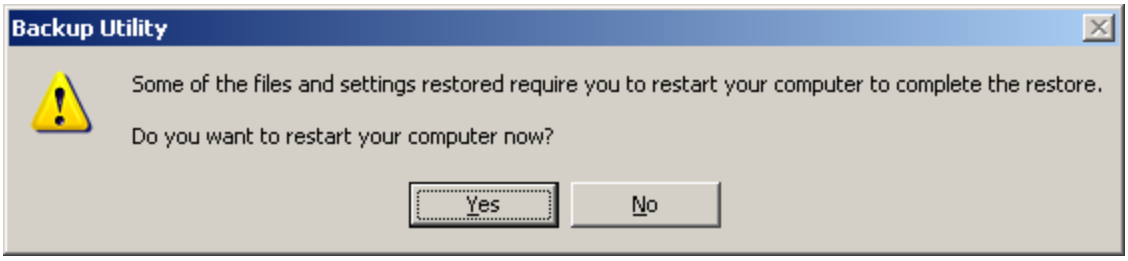
۸. صبر نمایید تا سیستم اطلاعات را Recovery کند.



۹. در این مرحله باز گردانی پشتیبان پایان می پذیرد. بر روی Close کلیک کنید.



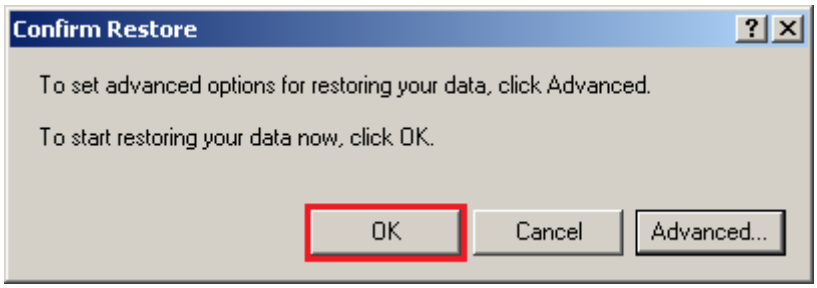
۱۰. در پنجره Backup Utility پیغامی مبنی بر شروع مجدد سیستم ظاهر می شود که شما Yesرا انتخاب کنید.



۱۹-۵-۳- نحوه بازگرداندن به صورت Normal

برای بازگرداندن پشتیبان مراحل زیر را طی کنید:

مانند روش باز گردانی Primary، مراحل را طی نمایید تا پنجره Confirm Restore باز شود. اما این بار روی دکمه OK کلیک کنید.

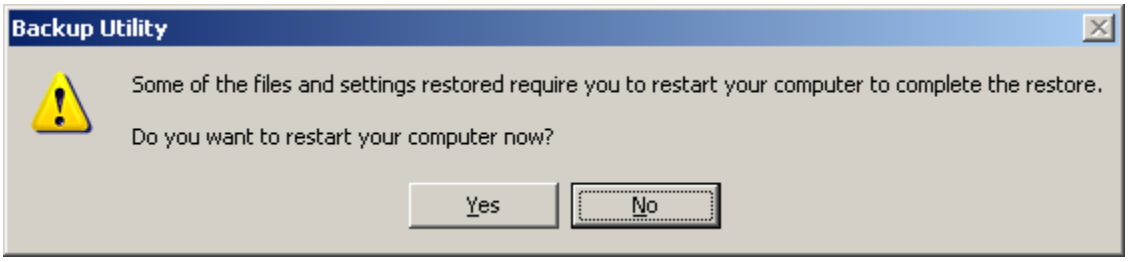


بقیه مراحل مانند روش Primary می باشد.

۱۹-۵-۴- نحوه بازگرداندن به صورت Authoritative

۱. مانند روش باز گردانی Normal، مراحل را طی نمایید (یعنی در صفحه Confirm Restore روی OK کلیک کنید) و ادامه دهید تا پنجره Backup Utility باز شود

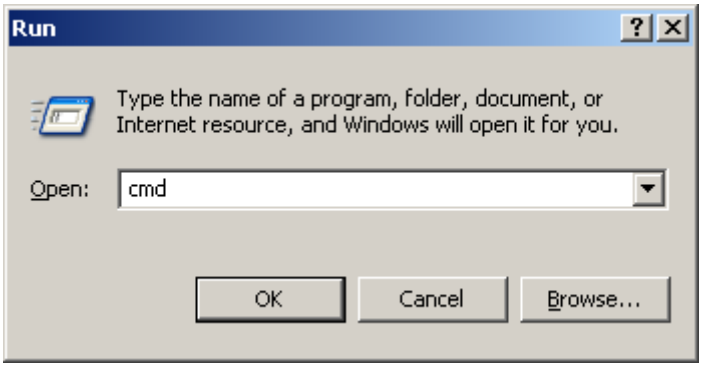
۲. در پنجره Backup Utility پیغامی مبنی بر شروع مجدد سیستم ظاهر می شود، که بر عکس شیوه Normal می بایست No را انتخاب کنید.



تفاوت شیوه Normal با Authoritative از همین مرحله آغاز می شود که یک سری داده را برای جلوگیری از بازنویسی در Replicate بین DC ها نشانه دار می کنید.

۳. از منوی Start برنامه CMD را از آدرس زیر اجرا کنید.

Start ➔ Run ➔ Enter 'CMD' ➔ OK



۴. در خط فرمان Ntdsutil را اجرا کنید. سپس در اعلان Ntdsutil، عبارت Authoritative Restore را تایپ و اجرا کنید.

توجه: در اعلان Authoritative Restore برای نشانه گذاری بدین ترتیب عمل کنید:

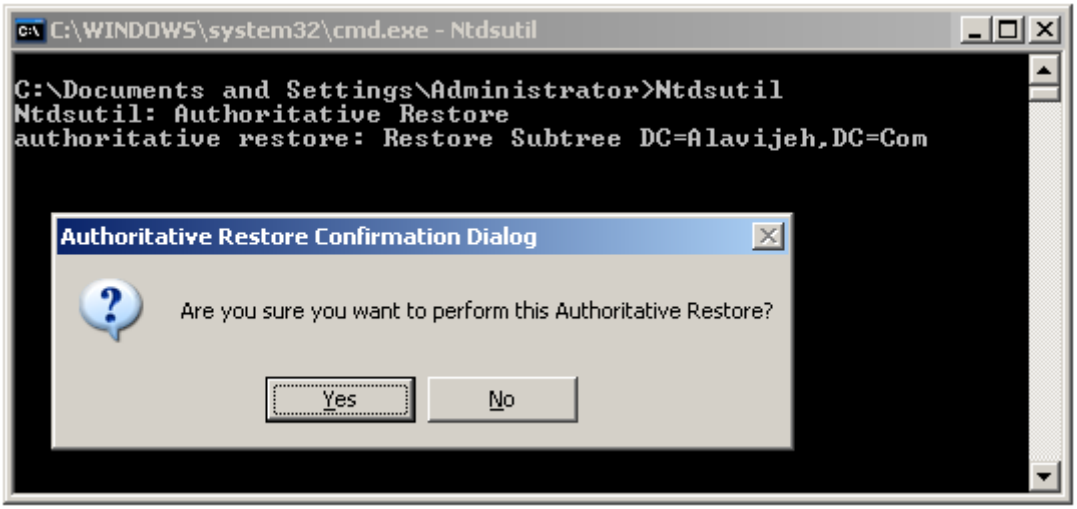
Restore SubTree Distinguished_Name_Of_Object

Distinguished Name، آدرس عنصر (Object) مورد نظر در Active Directory می باشد.

برای مثال برای نشانه گذاری دامنه Alavijeh.Com که در برای آزمایش حذف کرده بودید، بدین ترتیب عمل می کنیم:

Restore Subtree DC=Alavijeh,DC=Com

سپس در پنجره ظاهر شده Yes را انتخاب کنید.



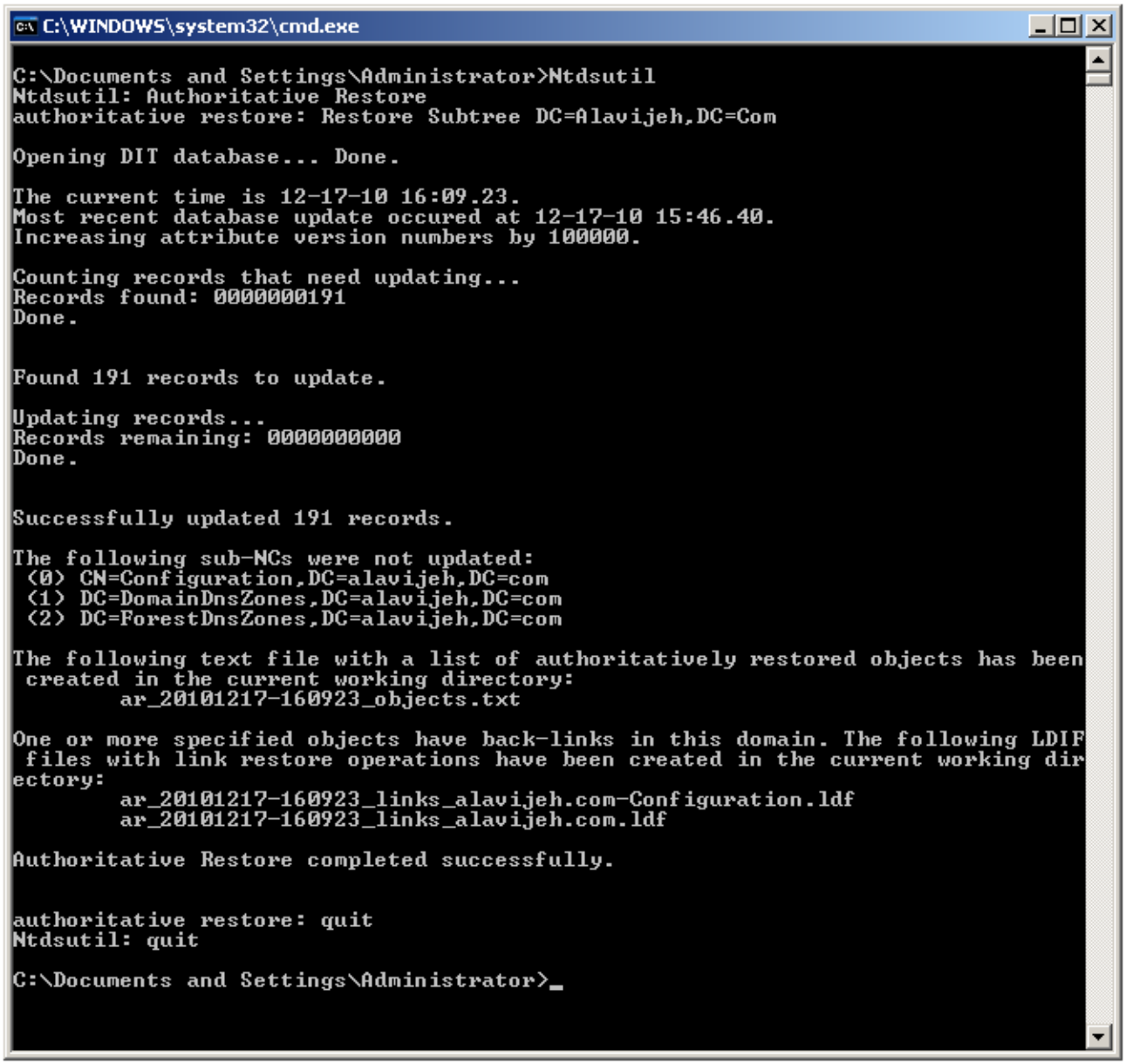
نکته: نشانه گذاری کل پایگاه داده و تنظیمات به صورتAuthoritative به این نحو انجام می شود:

Restore Database

۵. Object مورد نظر با موفقیت نشانه گذاری شد، حال دو مرتبه quit را تایپ و اجرا کنید تا از اعلان ntdsutil خارج شوید.

توجه داشته باشید که Objectی همانند OU به همراه تمامی Objectهای دیگری که در بر دارد مانند گروه ها و کاربر هایش نشانه گذاری می شود.

به شکل صفحه بعد دقت نمایید.



۶. Domain Controller را شروع مجدد کنید (Restart) و سیستم عامل را در حالت عادی اجرا کنید.

فصل ۲۰

DHCP Server

۲۰-۱- آشنایی با DHCP Server

DHCP Server به شما امکان می دهد تا آدرس های IP، Gateway، DNS، Subnet Mask، WINS و... را به صورت اتوماتیک از سرور دریافت کنید. در واقع اگر کارت شبکه ی شما در حالت خودکار تنظیم شده باشد، هنگام بوت شدن، درخواستی را به DHCP Server ارسال کرده و آدرس های مورد نیاز خود را دریافت می کند. به این صورت تمامی روند دادن آدرس IP به صورت خودکار انجام خواهد شد. یک ایستگاه کاری (Client) در شبکه برای اتصال به سرور و تماس با دیگر کامپیوتر ها نیاز به یک آدرس منطقی به نام آدرس IP دارد. وقتی در یک شبکه محلی تعداد زیادی کامپیوتر وجود داشته باشد، یک مدیر شبکه امکان تخصیص و تنظیم آدرس IP برای همه آنها به صورت دستی را نخواهد داشت و وقت بسیار زیادی برای تنظیم آدرس IP تک تک ایستگاه ها صرف خواهد شد. سرویس DHCP این امکان را فراهم می آورد که یکی از سیستم ها (در اینجا سرور Windows 2003) به صورت اتوماتیک و بدون دخالت مدیر شبکه به سیستم های کاری یا Client ها آدرس IP اختصاص دهد. DHCP مخفف کلمات Dynamic Host Configuration Protocol است؛ یعنی پروتکل تنظیم پویای میزبان ها (Host). منظور از Host در این جمله همان کامپیوتر یا ایستگاه های داخل شبکه است.

۲۰-۱-۱- ویژگی های DHCP

۱. **جلوگیری از Conflict:** اگر به صورت حرفه ای با شبکه کار کرده باشید، حتما با پیغامی مبنی بر وجود دو آدرس IP یکسان در شبکه برخورد کرده اید. این اتفاق زمانی رخ می دهد که دو سیستم واقع در یک شبکه، از یک آدرس IP استفاده کنند. اما این مشکل با استفاده از DHCP حل خواهد شد و بدین ترتیب می توانیم مطمئن باشیم چنین اتفاقی نخواهد افتاد.

نکته: بعد از راه اندازی DHCP Server و با تنظیمات پیش فرض آن، باز هم احتمال رخ دادن Conflict وجود دارد.

۲. **سرعت بخشیدن به کارها:** در یک شبکه ی بزرگ که از DHCP استفاده نمی کنند، اگر شما بخواهید آدرس DNS Server را تغییر بدهید، چه اتفاقی می افتد؟ اتفاق خاصی نمی افتد ولی باید آدرس DNS تک تک سیستم ها را تغییر دهید. در صورتی که اگر یک DHCP Server در شبکه وجود داشته باشد، کافی است آدرس DNS مورد نظرتان را در آن وارد کنید.

۳. **مدیریت متمرکز:** که باز هم می توانیم مثال بالا را برای آن ذکر کنیم. به جای عوض کردن آدرس DNS تک تک سیستم ها، می توانید از طریق یک سیستم و به صورت متمرکز، به خواسته های خود جامه ی عمل بپوشانید.

۴. **ضرورت:** در بعضی از شرایط، مجبور به استفاده از DHCP Server ها هستیم. مثلاً هنگامی که شما از یک ISP اینترنت دریافت می کنید، مدیر آن برای دادن آدرس IP به منزل شما مراجعه نمی کند. تمامی این فرایند ها از طریق راه دور و البته DHCP Server صورت می گیرد.

۲۰-۱-۲- جایگاه سرویس دهنده DHCP در یک شبکه مبتنی بر ویندوز ۲۰۰۳

به منظور بکارگیری DHCP در یک محیط ویندوز ۲۰۰۳، از رویکردهای متفاوتی استفاده می گردد. با توجه به اینکه DHCP پروتکلی است که دارای محدودیت های امنیتی خاص خود است، سرویس DHCP نباید به خارج ارائه گردد. همچنین به Domain Server های حیاتی و ماشین های سرویس گیرنده مهم، می بایست آدرس های IP ثابتی نسبت داده شود که ارتباطی با DHCP نخواهد داشت. سرویس DHCP Client بر روی ماشین های حساس، غیرفعال گردد. در زمان نصب ویندوز ۲۰۰۳ (هم سرویس دهنده و هم سرویس گیرنده)، سرویس DHCP Client فعالیت خود را آغاز و به عنوان یک سیستم محلی اجراء خواهد شد. سرویس دهندگان DHCP و سایر ماشین های حساس دیگر که از آدرس های IP ثابتی استفاده می نمایند به این سرویس نیاز نداشته و لازم است که سرویس فوق، متوقف و وضعیت فعالیت آن در زمان راه اندازی سیستم به حالت دستی (Manually) تغییر یابد.

۲۰-۱-۳- پیکربندی سرویس دهنده DHCP

سرویس دهنده DHCP به صورت اتوماتیک آدرس های IP و سایر اطلاعات مرتبط با پیکربندی TCP/IP را در اختیار سرویس گیرندگان DHCP-Enabled، قرار می دهد. سرویس دهنده DHCP به عنوان یک سیستم محلی اجراء می گردد. به منظور کاهش احتمال بروز خرابی و اشکالات حاصل از عوامل جانبی، پیشنهاد می گردد که سرویس دهنده DHCP بر روی یک Domain Server که یک Domain Controller **نمی باشد**، نصب گردد. جایگاه سرویس دهندگان DHCP، بسیار حساس و مهم بوده و می بایست تمامی آنان دارای آدرس های IP ثابت باشند. سرویس DHCP Client می بایست برروی این نوع از سیستم ها متوقف و وضعیت اجراء آن در زمان راه اندازی سیستم، به صورت دستی در نظر گرفته شود.

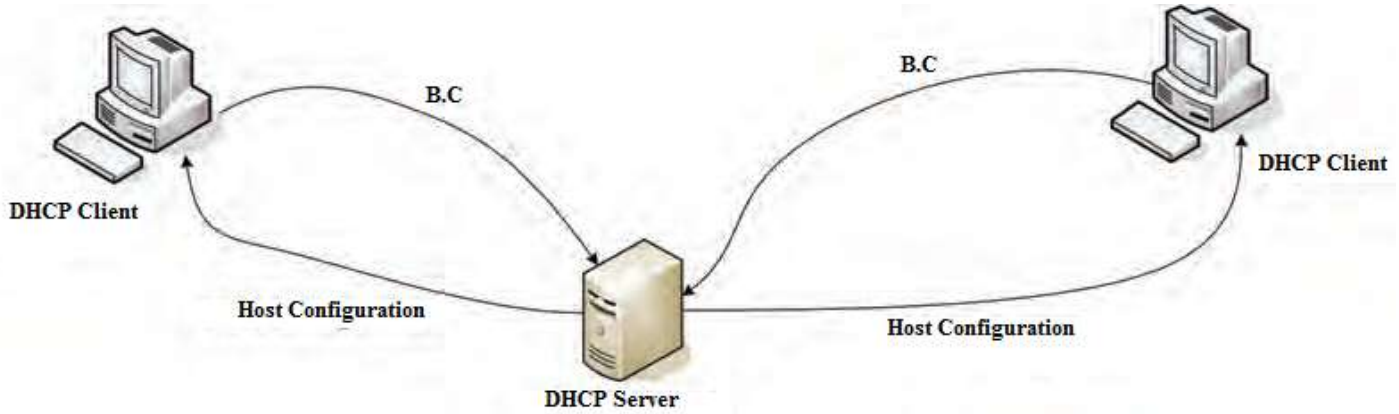
۲۰-۱-۴- پیکربندی سرویس گیرندگان DHCP

سرویس DHCP Client، به صورت اتوماتیک درخواست هایی را برای سرویس دهنده DHCP به منظور دریافت یک آدرس IP و نسبت دهی آن به ماشین سرویس گیرنده، انجام می دهد. درخواست فوق، در زمان راه اندازی سیستم (Booting) انجام و در صورت ضرورت و قبل از اتمام تاریخ اعتبار آن (نصف زمان تاریخ انقضاء)، تکرار خواهد شد. سرویس DHCP Client به عنوان یک سیستم محلی بر روی ماشین سرویس گیرنده اجراء خواهد شد. پیشنهاد می گردد که از خدمات DHCP بر روی ماشین های سرویس گیرنده حساس و مهم **استفاده نگردد**. این نوع از ماشین های سرویس گیرنده، می بایست از آدرس های IP ثابتی استفاده و بر روی آنان سرویس DHCP Client متوقف و نحوه راه اندازی آنان در زمان راه اندازی، به صورت دستی یا ایستا تعیین گردد.

منظور از DHCP Client، سرویسی است که در طی فرآیند راه اندازی (Boot)، با سرویس دهنده DHCP ارتباط برقرار کرده و پیکربندی لازم را از آن دریافت می کند. بدیهی است که این سرویس بایستی روی کلیه ایستگاه هایی که پیکربندی آن ها می خواهد به طور خودکار انجام شود، فعال گردد.

در سیستم عامل ویندوز، نسخه های XP، 2000، 2003، 2008، Vista و ۷، با مراجعه به کنسول سرویس ها (Services.msc)، می توان فعال بودن این سرویس را بررسی کرد. وضعیت سرویس باید در حالت Started باشد.

همانطور که از شکل زیر پیدا است، DHCP Client پس از فعال شدن روی ایستگاه ها با استفاده از Broadcast (به اختصار BC) سرویس دهنده را پیدا کرده و بعد از طی مراحلی کوتاه، پیکربندی لازم را از سرویس دهنده دریافت می کند.



حال چنانچه DHCP Server در شبکه نباشد و یا در زمان مناسب، به دلایلی مانند ترافیک، شبکه نتواند پاسخ لازم را به کلاینت بدهد، در آن صورت بسته به رفتار سیستم عامل کلاینت، ممکن است یکی از حالات زیر اتفاق بیفتد:

الف) سرویس گیرنده پیکربندی نمی شود. در سیستم عامل های مایکروسافت Win 95 و NT 4.0 چنین اتفاقی می افتد که با مراجعه به Command Prompt و وارد نمودن دستور ipconfig یا winipcfg می بینیم که آدرس به صورت 0.0.0.0 است و این موضوع نشان می دهد که آدرس IP در سرویس گیرنده پیکربندی نشده است.

ب) سرویس گیرنده به طور خودکار و تصادفی یک آدرس به خود می دهد. سیستم عامل های Me، Win 98، XP، 2000، 2003، 2008، Vista و ۷ چنین رفتاری دارند که با مراجعه به Command Prompt و وارد کردن دستور ipconfig یا winIPcfg می بینیم که آدرس تصادفی در محدوده 169.254.X.Y (یعنی از ۱۶۹.۲۵۴.۰.۱ تا ۱۶۹.۲۵۴.۲۵۵.۲۵۴) با Subnet Mask کلاس B یعنی ۲۵۵.۲۵۵.۰.۰ تنظیم شده است. به این روش تخصیص آدرس به صورت تصادفی، اصطلاحا APIPA (Automatic Private IP Addressing) می گویند. البته کلاینت بعد از انتخاب یک آدرس تصادفی، با دیگر کلاینت های موجود در شبکه برای بررسی تکراری بودن آدرس IP مذاکره می کند.

متاسفانه روش APIPA مکانیزم مناسبی برای پیکربندی در شبکه ها نیست. زیرا:

- غیر از IP و Subnet Mask، پارامتر دیگری را تنظیم نمی کند (از قبیل Router یا DNS)
- ترافیک شبکه را افزایش می دهد (می خواهد بررسی کند که آیا آدرس تکراری است یا خیر)
- غیر از محدوده 169.254.X.Y، محدوده دیگری را نمی توان روی آن تنظیم کرد. به عبارت دیگر، APIPA قابل تنظیم نیست.

نکته: در فرآیند APIPA، پس از آن که سرویس گیرنده آدرس را به صورت تصادفی برای خود انتخاب کرد، آن را تا مدت کوتاهی (حدود ۵ دقیقه) نگه داشته و سپس مجددا به دنبال DHCP Server می گردد؛ که البته این جستجو با Broadcast انجام می شود. حال اگر بتواند از آن جواب بگیرد، در آن صورت پیکربندی خود را طبق دستور العمل سرویس دهنده انجام می دهد و در غیر اینصورت، یعنی نگرفتن پاسخ از DHCP Server، همان آدرس تصادفی قبلی را استفاده می کند و این فرآیند مرتبا تکرار می شود؛ یعنی حدوداً هر ۵ دقیقه یکبار، به روش Broadcast به دنبال DHCP Server می گردد و این امر افزایش ترافیک بیش از حد در شبکه های متوسط و بزرگ را به همراه خواهد داشت.

ج) سرویس گیرنده به طور خودکار با آدرس از پیش تعیین شده تنظیم شود. در سیستم عامل ویندوز نسخه های XP و ۲۰۰۳ (و نسخه های جدید تر) چنین قابلیتی وجود دارد که اگر سرویس گیرنده ای، DHCP Server را پیدا نکند، با آدرس و سایر پارامتر های دیگری که از قبل تعریف شده است، خود را تنظیم کند. این حالت اصطلاحا Alternate Configuration نام دارد.

۲۰-۲- نصب DHCP Server

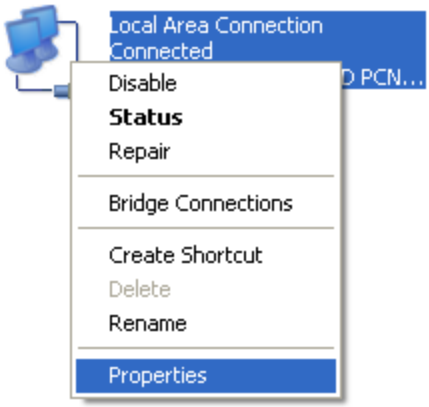
قبل از اینکه اقدام به نصب DHCP نماییم، لازم است حداقل یک IP Address به صورت Static یا دستی برای دستگاهی که قرار است سرویس DHCP را برای شبکه فراهم آورد تعریف کرد. این دستگاه در این بحث، همان ویندوز سرور ۲۰۰۳ می باشد. در صورتیکه این کار انجام نپذیرد، در هنگام نصب DHCP، سیستم مذکور پیغام زیر را می دهد.

۲۰-۲-۱- تنظیم IP Address برای سرور (به صورت دستی)

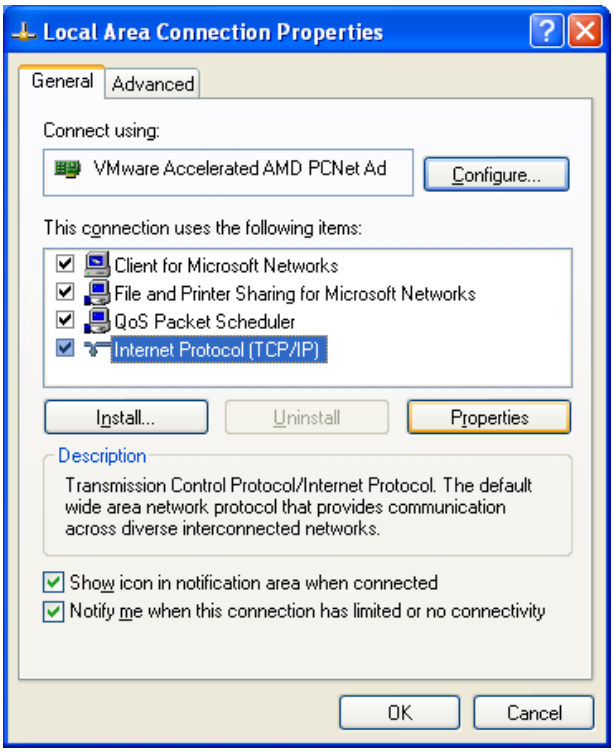
از مسیر زیر پنجره Local Area Connection را باز کنید (البته چندین راه برای این کار وجود دارد).

Start ➔ Control Panel ➔ Network Connections ➔ Local Area Connection

روی گزینه Local Area Connection راست کلیک کرده و گزینه Properties را انتخاب کنید تا پنجره Local Area Connection Properties فعال گردد.



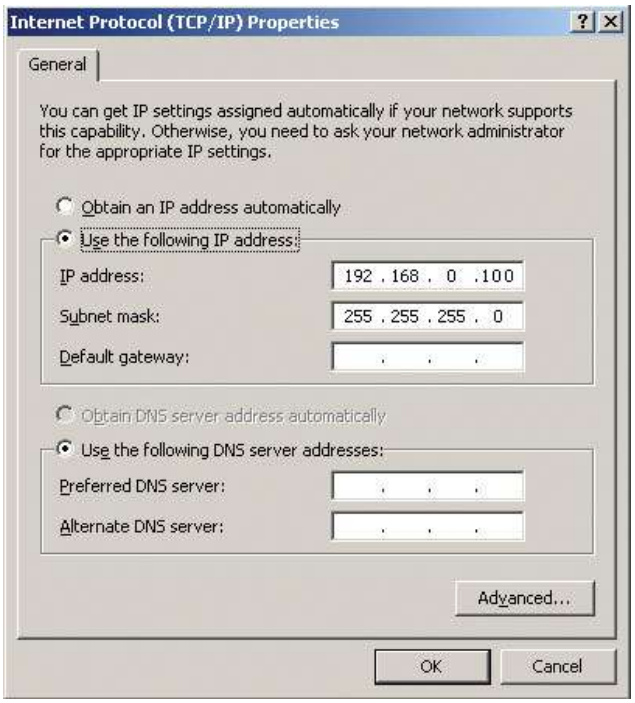
در شکل زیر، گزینه Internet Protocol (TCP/IP) را انتخاب و دکمه Properties را بزنید تا پنجره Internet Protocol (TCP/IP) Properties باز شود.



مطابق شکل زیر، می توانید آدرسIP که قبلاً بررسی و انتخاب نموده اید را وارد نمائید. (مثلاً ۱۹۲.۱۶۸.۰.۱۰۰)

در این صفحه، دو قسمت Subnet Mask و Default Gateway را نیز می توانید تنظیم نمایید. (تنظیم Subnet Mask ضروری است، ولی تنظیم Default Gateway اختیاری است)

در پایان این قسمت دکمه OK را بزنید.



اکنون سرور دارای یک IP Address می باشد و می توانید برای نصب DHCP Server اقدام نمائید.

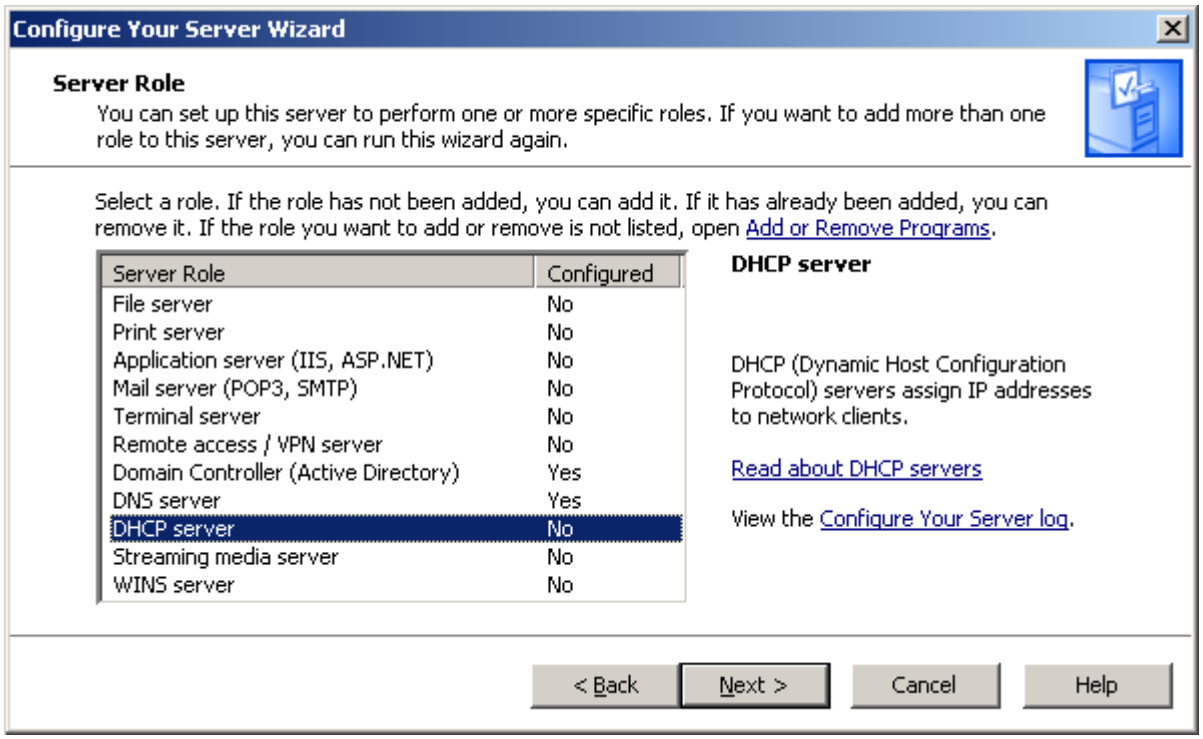
۲۰-۲-۲- نصب DHCP Server

برای شروع نصب، در ویندوز سرور وارد مسیر Start ➔ Administrative Tools ➔ Configure Your Server Wizard شوید.

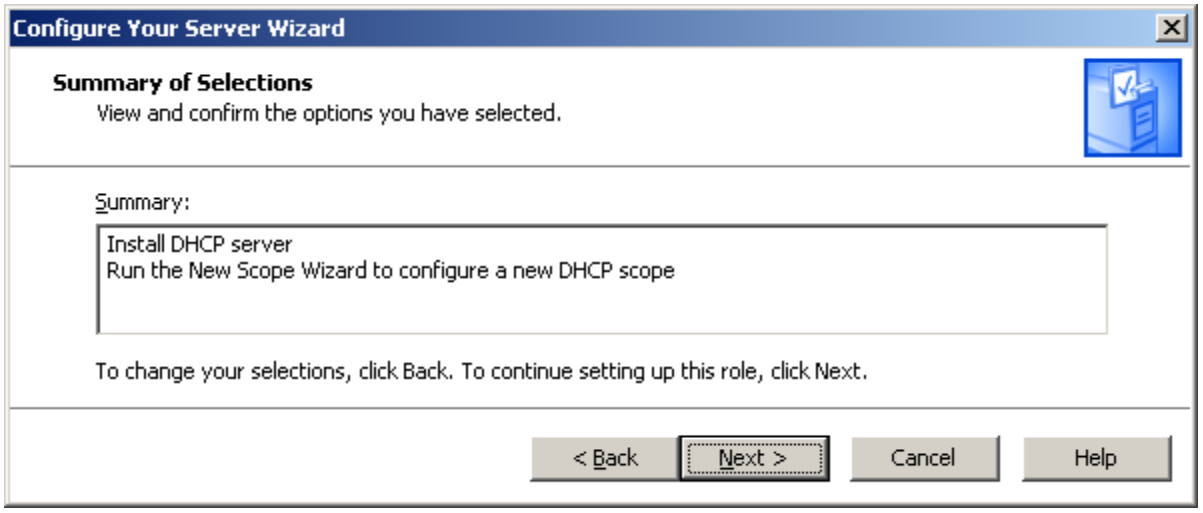
در صفحه خوش آمد گویی، دکمه Next را بزنید.

مجددا Next را بزنید.

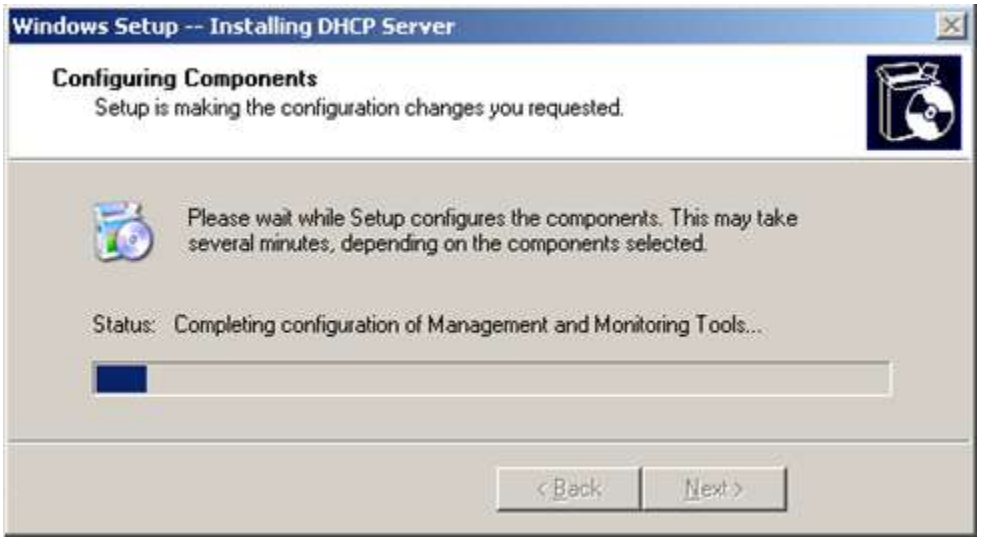
در صفحه باز شده، گزینه DHCP Server را انتخاب کنید، این بدان معناست که می خواهید نقش DHCP Server را به این کامپیوتر بدهید. سپس روی دکمه Next کلیک کنید.



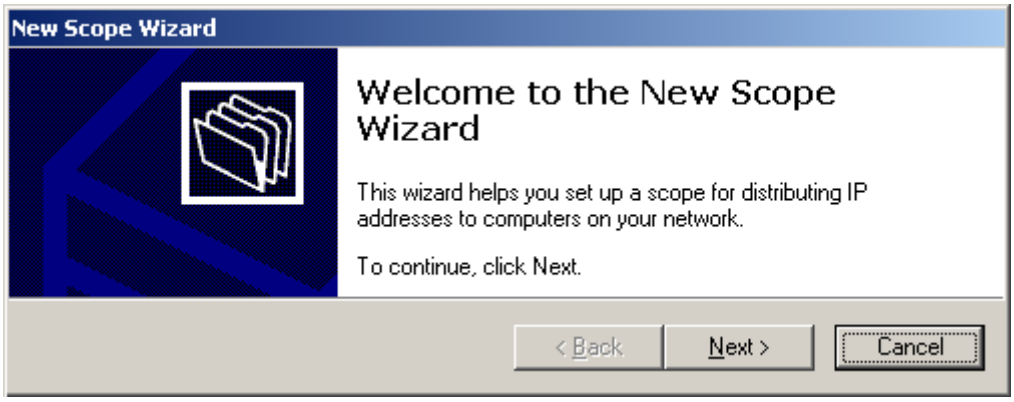
مجددا روی دکمه Next کلیک کنید.



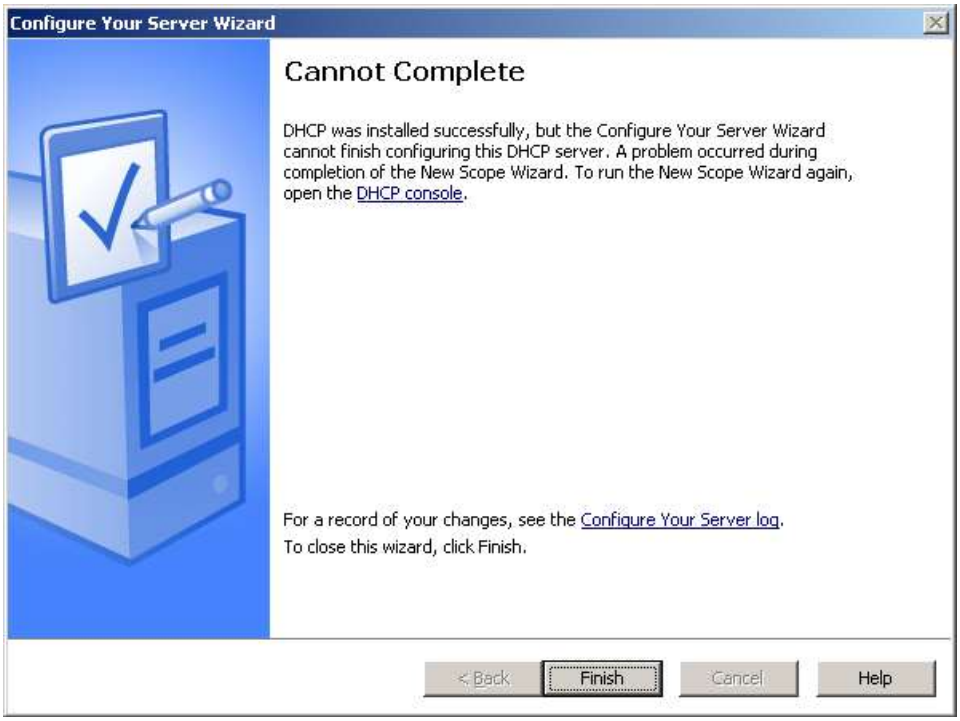
صبر کنید تا سیستم، DHCP Server را نصب کند. در صورتی که سیستم از شما CD ویندوز را خواست، آن را در دستگاه قرار دهید.



در مرحله بعد، سیستم می خواهد تنظیماتی را انجام دهد. اما فعلا دکمه Cancel را انتخاب نمایید. زیرا ما قصد داریم این کار را به صورت دستی انجام دهیم.



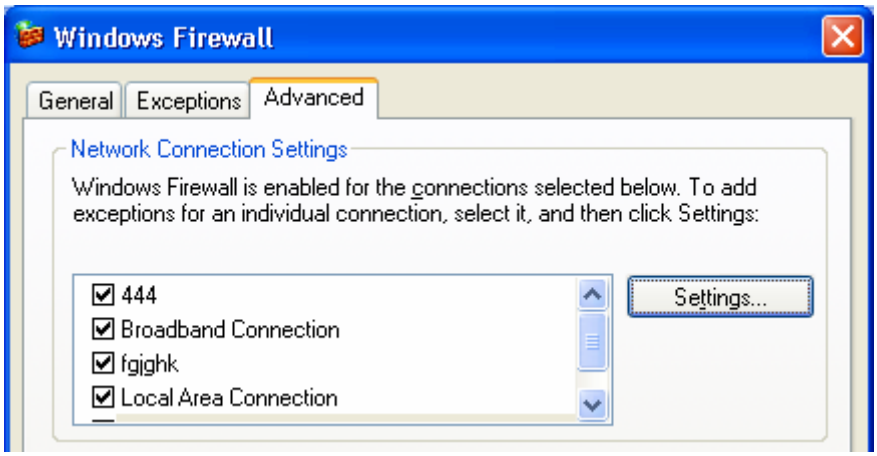
روی دکمه Finish کلیک کنید. توجه نمایید که تا اینجا، عملیات نصب به صورت ناقص انجام شده است. چگونگی تکمیل فرآیند نصب را جلوتر توضیح می دهیم.



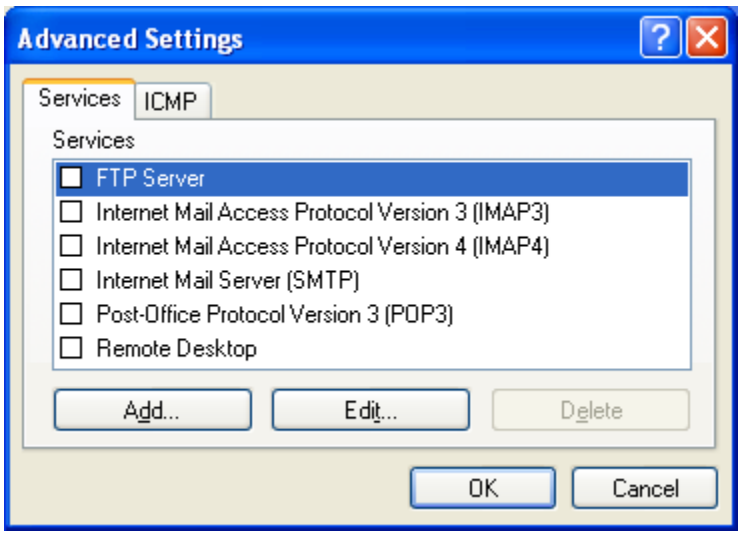
۲۰-۲-۳- پیکربندی *Firewall*

در این مرحله، نوبت به پیکربندی Firewall جهت قادر ساختن آن به منظور دریافت درخواست Clientها برای آدرس IP می باشد. یعنی باید به Firewall بگوییم که درخواست های تخصیص IP را Reject (رد درخواست) نکند. بدین منظور، ابتدا از طریق Control Panel وارد Windows Firewall شوید. البته اگر Firewall شما غیر فعال باشد، نیازی به تنظیم این بخش نیست.

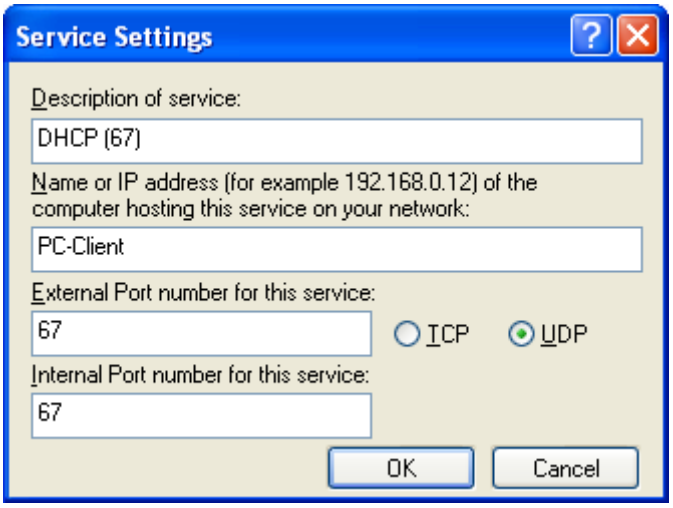
کاری که شما بایستی انجام دهید، این است که به Firewall بگویید که درخواست های DHCP را رد نکند. این درخواست ها از طریق پورت شماره ۶۷ و به صورت UDP وارد می شود. برای تنظیم این مورد، پس از باز شدن Windows Firewall، وارد سربرگ Advanced شده و سپس روی دکمه Settings کلیک کنید.



سپس در صفحه باز شده، برای افزودن پورت شماره ۶۷، روی دکمه Add کلیک کنید.

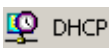


سپس در صفحه باز شده، در جعبه متن اول، نامی دلخواه برای این سرویس وارد نمایید. در جعبه متن دوم، نیز نام کامپیوتر یا آدرس IP کامپیوتری که این سرویس روی آن قرار دارد را وارد نمایید. در دو جعبه متن باقیمانده، عدد ۶۷ را وارد نمایید (عدد ۶۷ بیانگر شماره پورتی است که برای DHCP استفاده می شود). در قسمت آخر نیز UDP را انتخاب نمایید. زیرا روش انتقال درخواست DHCP به صورت UDP می باشد. در نهایت روی OK کلیک کنید.



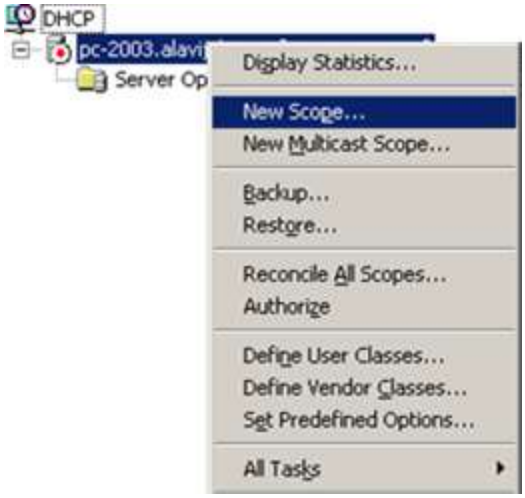
۲۰-۳- پیکربندی DHCP Server

برای پیکربندی، از منوی Start، منوی Administrative Tools، گزینه DHCP را انتخاب نمایید.



با این کار پنجره DHCP باز می شود.

برای شروع پیکربندی، ابتدا بایستی یک Scope را ایجاد نمایید. در مباحث تئوری DHCP، گفتیم که DHCP Server، به Clientها آدرس IP تخصیص می دهد. DHCP Server، بایستی آدرس IP را بر اساس قواعدی مشخص انتخاب نماید و نمی تواند آن را بدون نظم (به قول شیرازی ها : هِرِلی) انتخاب نماید. بدین منظور ما بایستی یک Scope تنظیم نماییم. منظور از Scope، محدوده ای از آدرس های IP است که DHCP Server، IP ها را از این محدوده انتخاب خواهد کرد. برای ساخت Scope جدید، روی نام سرور راست کلیک کرده و گزینه New Scope را انتخاب نمایید.



یک Wizard برای تعریف Scope شامل دو بخش است:

الف) مشخصات اولیه شامل:

- **Name Description**: یک نام یا توضیح دلخواه است که برای توصیف Scope استفاده می باشد.
- **IP Address Range Assigned to Client & Subnet Mask**: بیانگر محدوده آدرسی می باشد که آدرس کلاینت ها از این محدوده انتخاب می شود. آدرس شروع و پایان محدوده بایستی هر دو در یک کلاس آدرس IP باشند.
- **IP Address Range Excluded (Not Assign to Clients)**: محدوده آدرسی است هیچ آدرسی از داخل آن، نباید به کاربر داده شود. این محدوده بایستی جزئی از محدوده قبلی باشد.
- **Lease Duration**: مدت زمانی است که اطلاعات پیکربندی به کلاینت اجاره داده می شود. البته زمانی که مدت دریافت اطلاعات کلاینت به نصف زمان اجاره برسد، کلاینت نسبت به تمدید آن اقدام می کند.

ب) مشخصات ثانویه (معروف به Scope Options) که شامل موارد زیر می باشد:

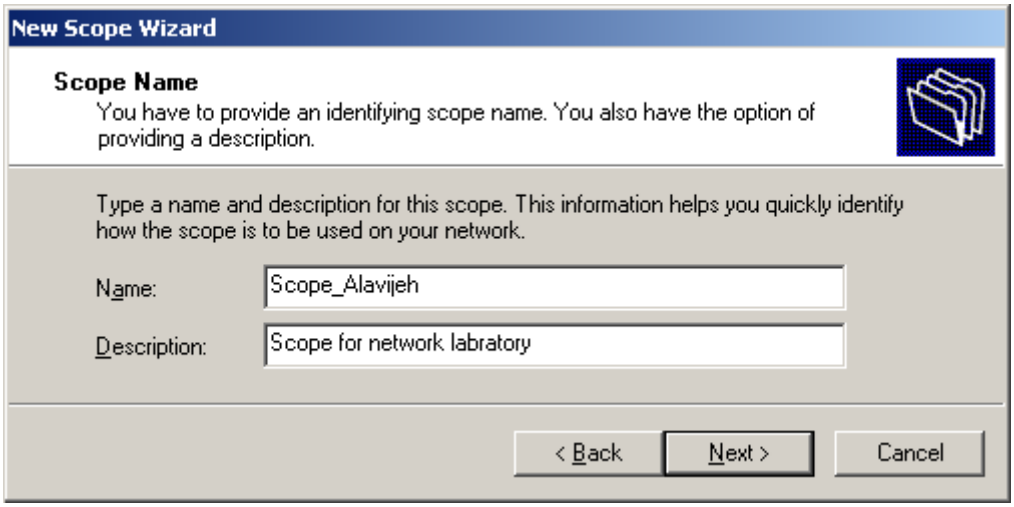
- **Router IP Address (Default Gateway)**: آدرس روتری است که کلاینت ها به واسطه آن به شبکه های دیگر راه پیدا می کنند. در رایانه های مبتنی بر سیستم عامل ویندوز، این پارامتر تحت عنوان Default Gateway شناخته می شود.
- **DNS Server IP Address**: آدرس کامپیوتری است که عملیات تبدیل نام کامپیوتر به آدرس IP را انجام می دهد.
- **Domain Name**
- **Win Server IP Address**

Node Type –

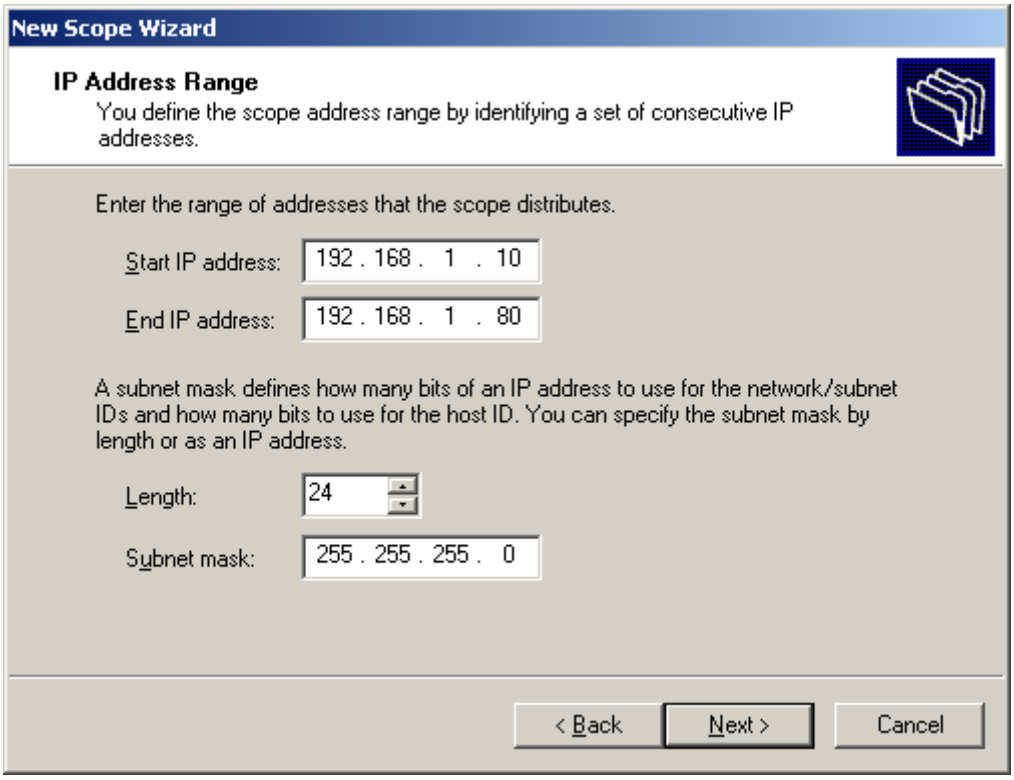
سه مورد فوق در حالت های خاص استفاده می شوند. لذا وارد جزئیات نمی شویم.

در صفحه باز شده، Next را بزنید.

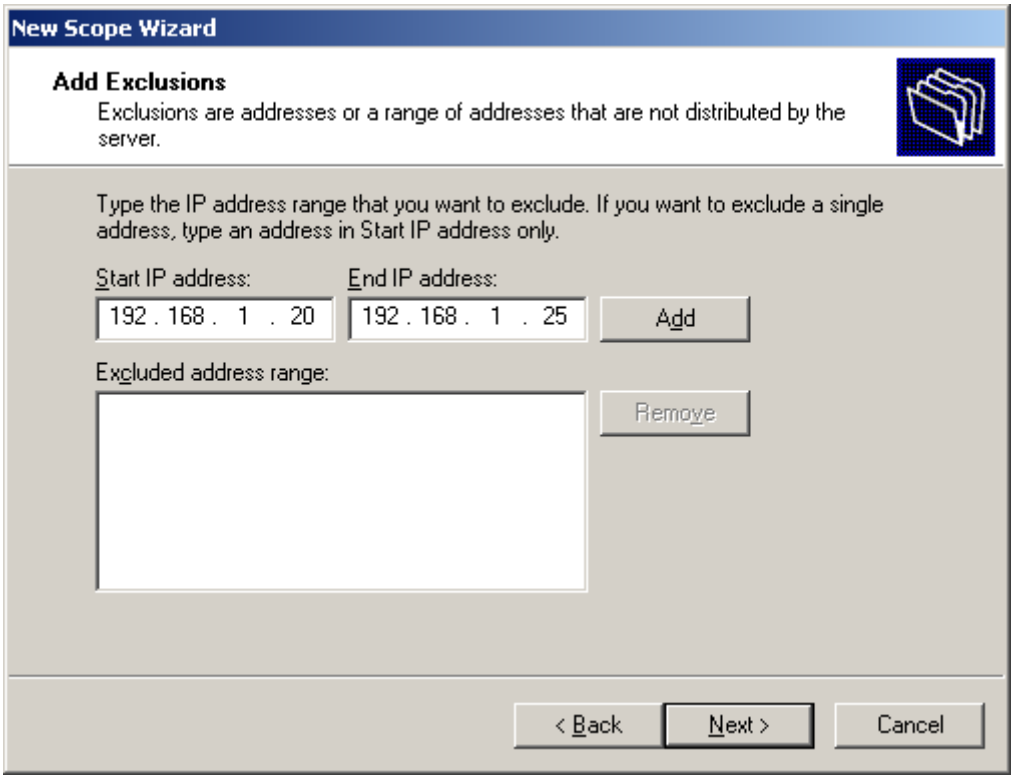
در صفحه بعدی، یک نام برای Scope به همراه یک توصیف (Description) برای آن Scope وارد نمایید.



در صفحه بعد، در قسمت Start IP Address، شروع محدوده IP و در قسمت End IP Address، پایان محدوده IP را وارد نمایید. قسمت پایین نیز، بخش Length بیانگر تعداد ۱ های Subnet Mast است (مفهوم Subnet Mast را در فصول قبل توضیح داده ایم). با تغییر مقدار Length، عدد مربوط به Subnet Mask در زیر آن تغییر خواهد کرد.

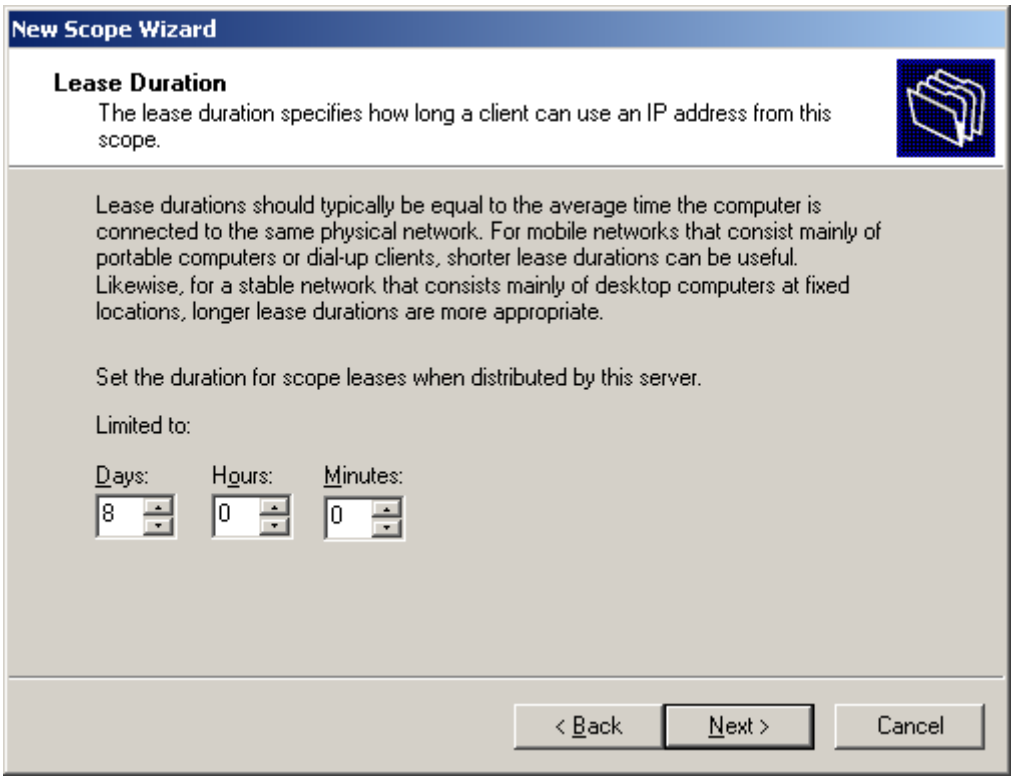


در صفحه بعد، می توانید محدوده IPای را وارد نمایید که قصد دارید DHCP Server آن را به Clientها تخصیص ندهد. به عبارت دیگر آن را Exclude نماید.

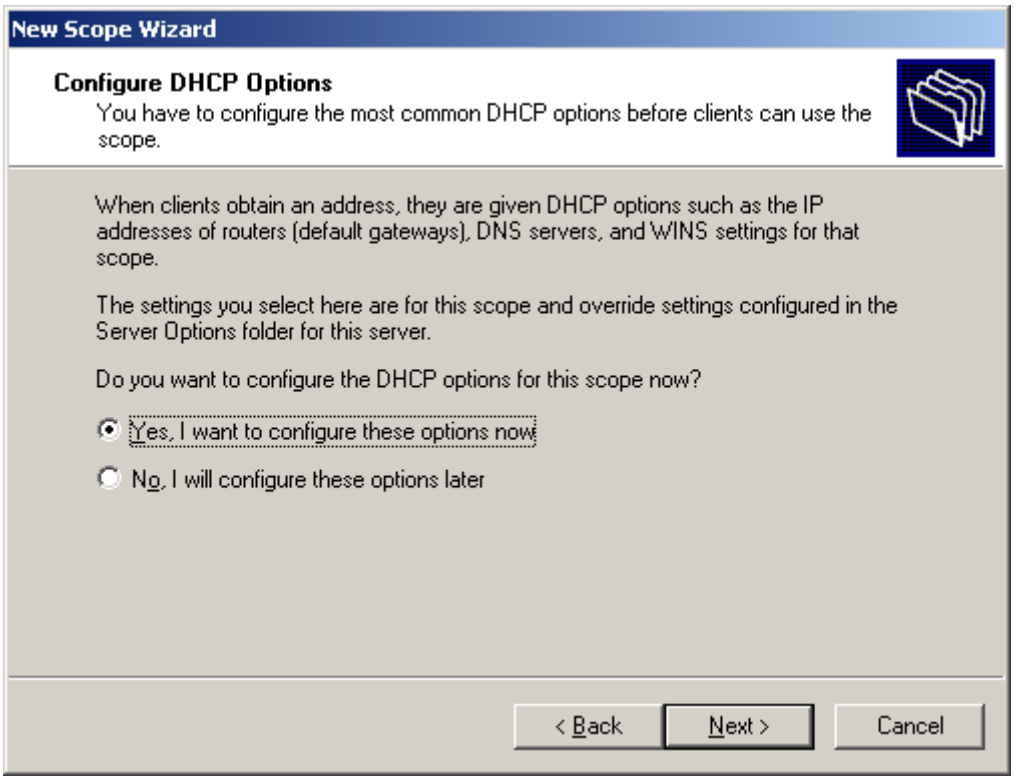


در صفحه بعدی، مدت زمانی که یک آدرس IP تخصیص داده شده معتبر خواهد بود را تعیین می کند. البته زمانی که نصف این زمان بگذرد، Client درخواست تمدید IP Address می کند. طول این زمان به طور پیش فرض ۸ روز است. اما می توان گفت که چنان چه در یک شبکه میزان جابجایی رایانه ها نسبتا کم باشد و از طرفی نیز محدوده آدرس نسبت به رایانه ها زیاد تر باشد، در آن صورت مدت زمان اجاره را طولانی انتخاب کنید و در صورتی که جابجایی رایانه ها زیاد باشد (مثلاً می خواهیم ایستگاه های قدیمی را از رده خارج کرده و ایستگاه های جدیدی جایگزین کنیم و یا به عنوان مثال تعداد رایانه های Notebook که به شبکه وارد می شوند و از آن خارج می گردند زیاد است) و از طرفی محدوده آدرس ها نسبت به تعداد رایانه

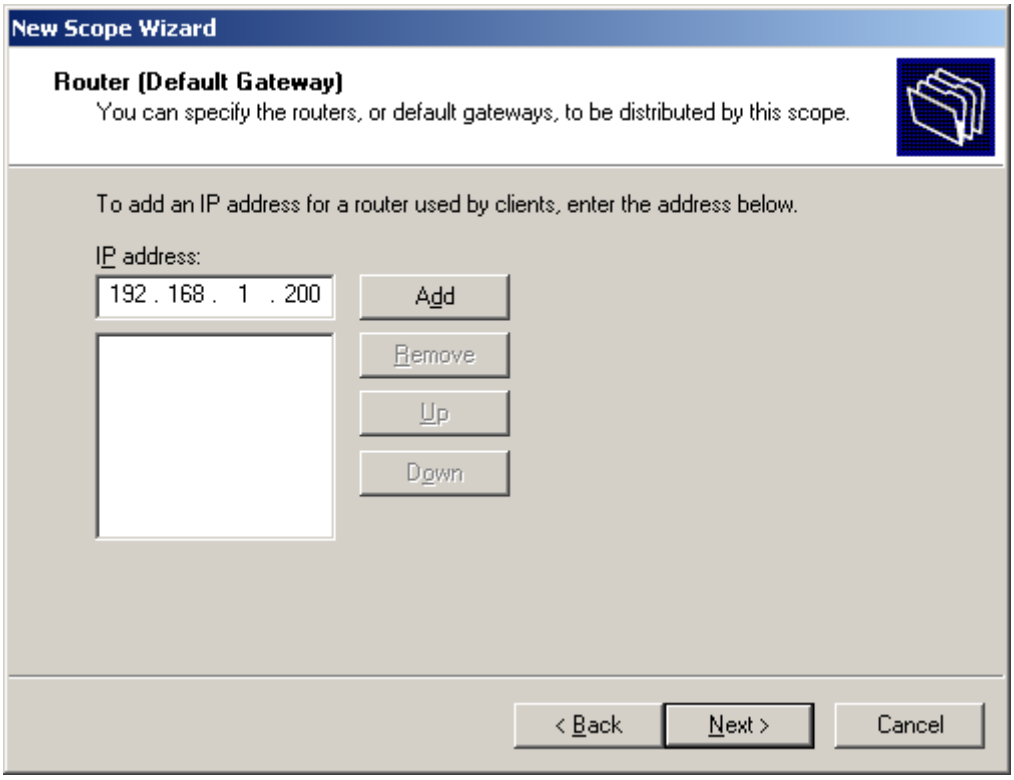
ها محدود باشد، در اینصورت مدت زمان اجاره را کوتاه انتخاب می کنیم. به بیانی دقیق تر مدت زمان اجاره بستگی به میـزان عرضه و تقاضای آدرس IP دارد. هر چه نسبت عرضه به تقاضا بیشتر باشد، مدت زمان را طولانی تر و هر چه نسبت عرضـه بـه تقاضا کمتر باشد، مدت زمان را کوتاه تر انتخاب می کنیم.



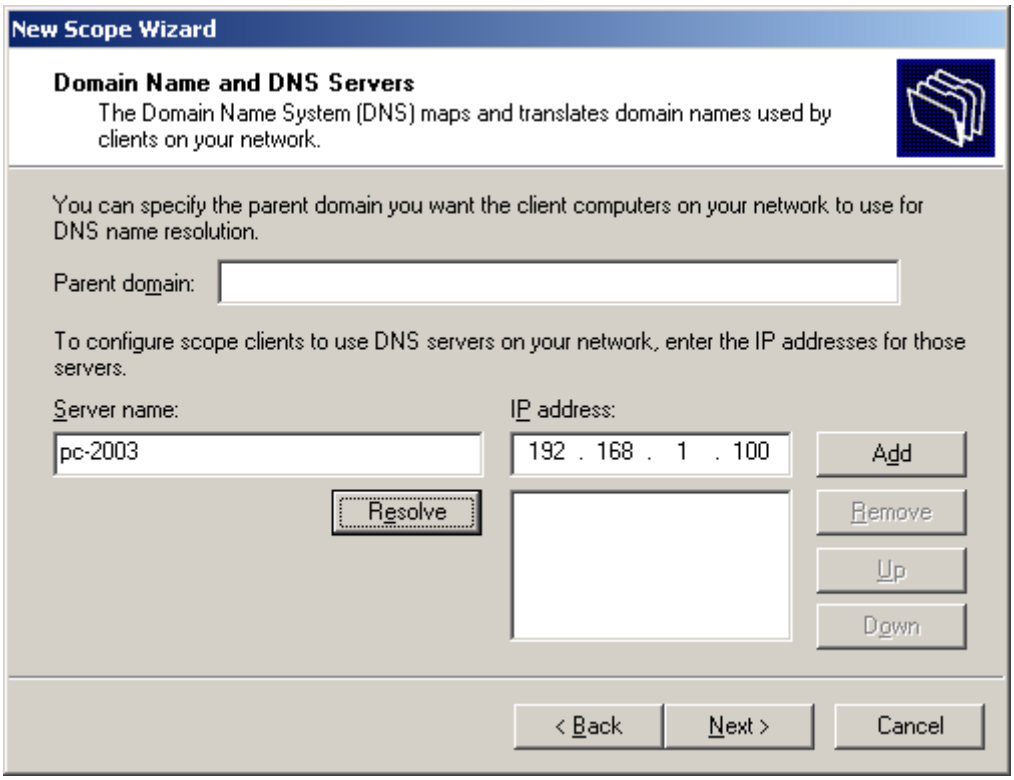
در صفحه بعدی تعیین نمایید که می خواهید تنظیمات دیگری را نیز انجام دهید.



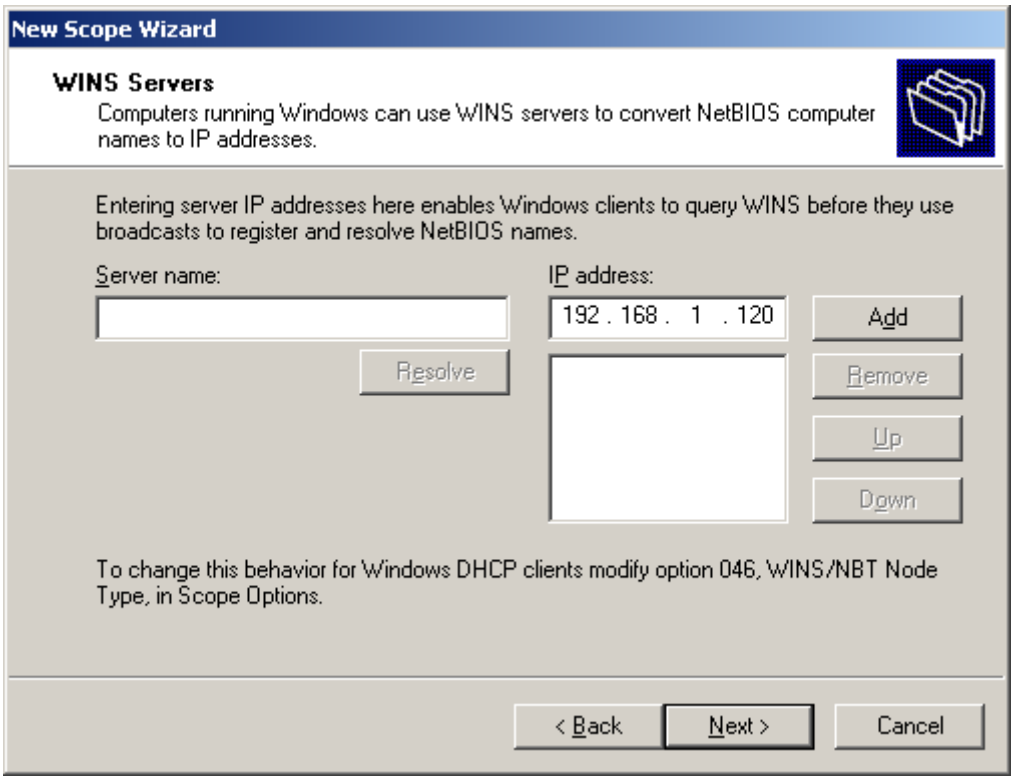
در صفحه بعدی، آدرس IP مربوط به Router یا Gateway پیش فرض را وارد نمایید.Gateway کـامپیوتری اسـت کـه بسـته های ارسالی ما، ابتدا به سمت آن می رود و وجود آن در شبکه اختیاری است.



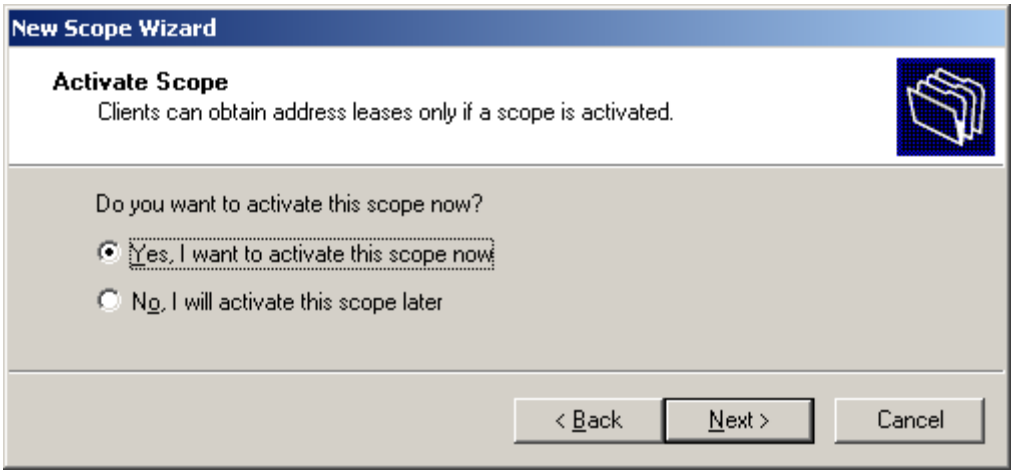
در صفحه بعد، آدرس IP مربوط به DNS Server را وارد نمایید. DNS Server وظیفه تبدیل اسامی Host Name به آدرس IP را بر عهده دارد. اگر آدرس IP را نمی دانید، نام DNS Server را وارد کرده و سپس روی دکمه Resolve کلیک نمایید. با این کار، DHCP Server آدرس DNS Server را نیز به Clientها می دهد.



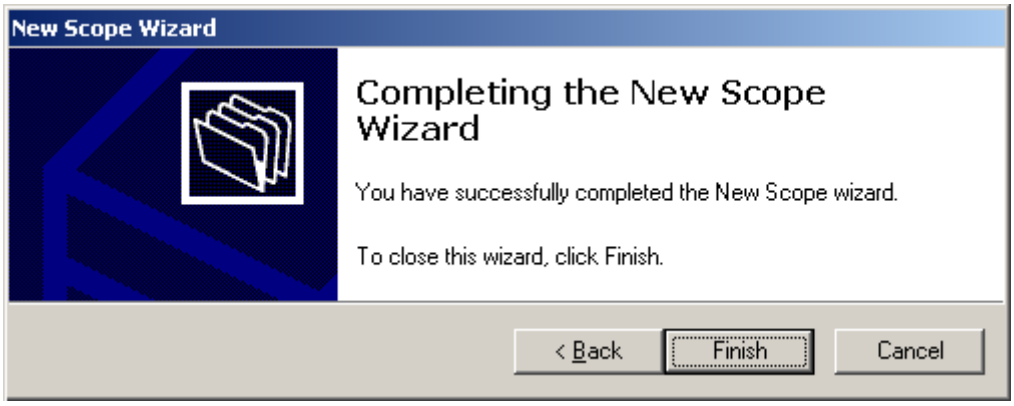
در صفحه بعد، آدرس IP مربوط به WINS Server را وارد نمایید. WINS Server وظیفه تبدیل اسامیNetBIOS Name به آدرس IP را بر عهده دارد. (برای اطلاعات بیشتر به فصل DNS Server مراجعه نمایید.)



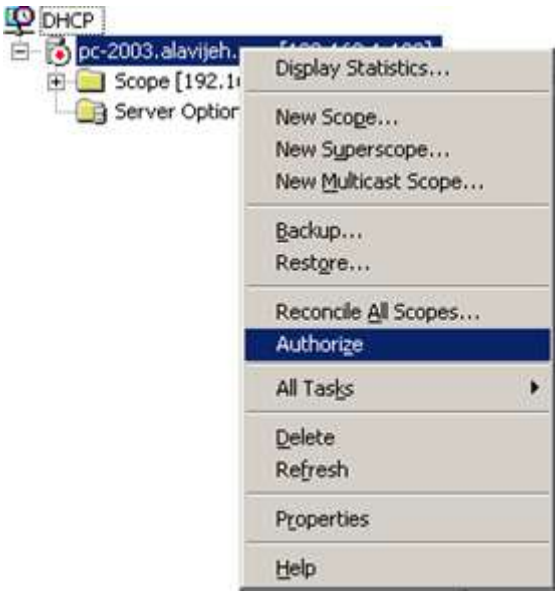
در صفحه بعد تعیین نمایید که قصد دارید این Scope را فعال نمایید.



سپس برای پایان نصب، روی دکمه Finish کلیک نمایید.



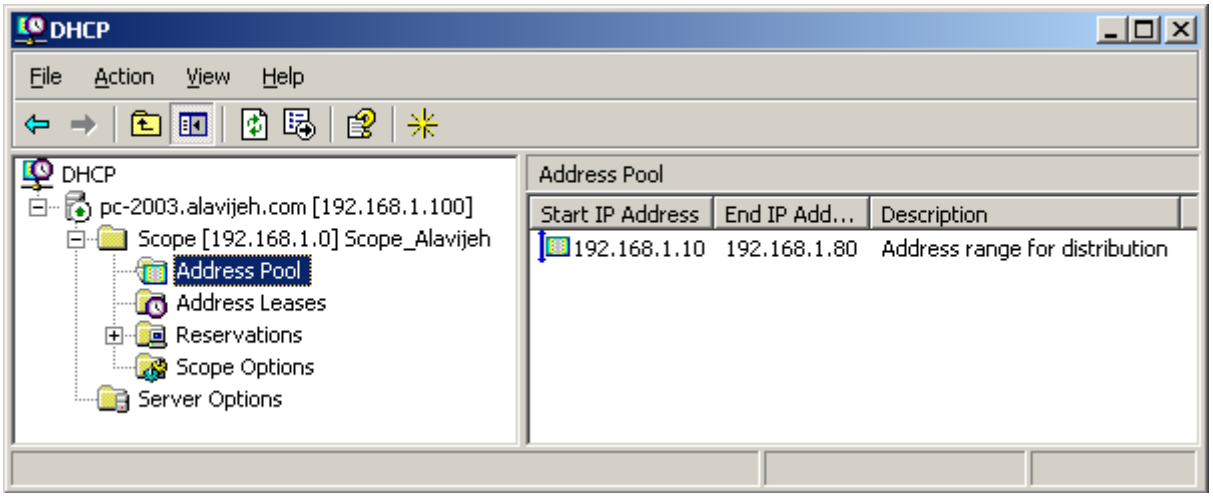
تا این مرحله، Scope ساخته شده فعال است. اما هنوز خود DHCP Server فعال (Authorize) نشده است. باید حتما DHCP Server خود را فعال کنید. این کار برای جلوگیری از تداخل وجود چند DHCP Server در شبکه است. بدین منظور در صفحه DHCP، روی نام سرور راست کلیک کرده و گزینه Authorize را انتخاب نمایید.



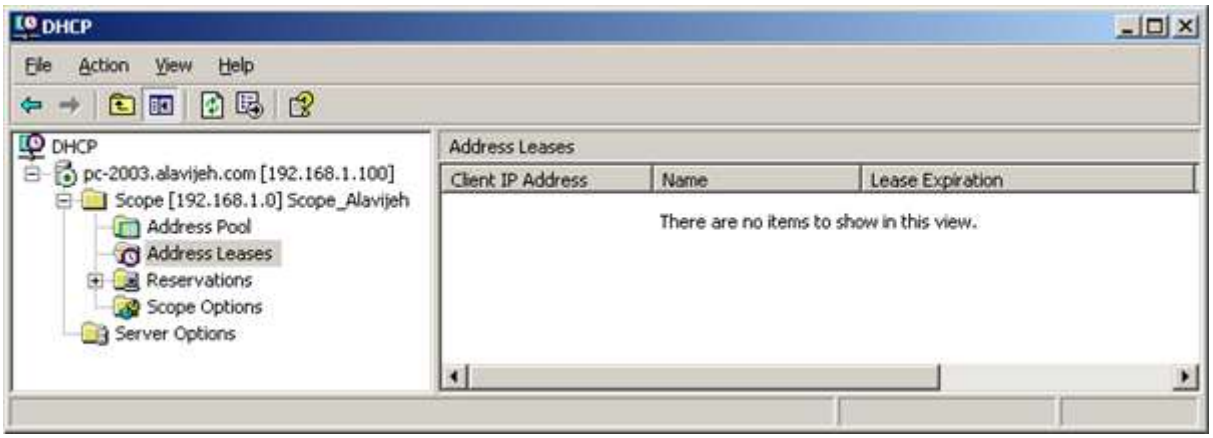
۲۰-۳-۱- قسمت های مختلف DHCP Server

در ادامه به معرفی قسمت های مختلف DHCP Server می پردازیم.

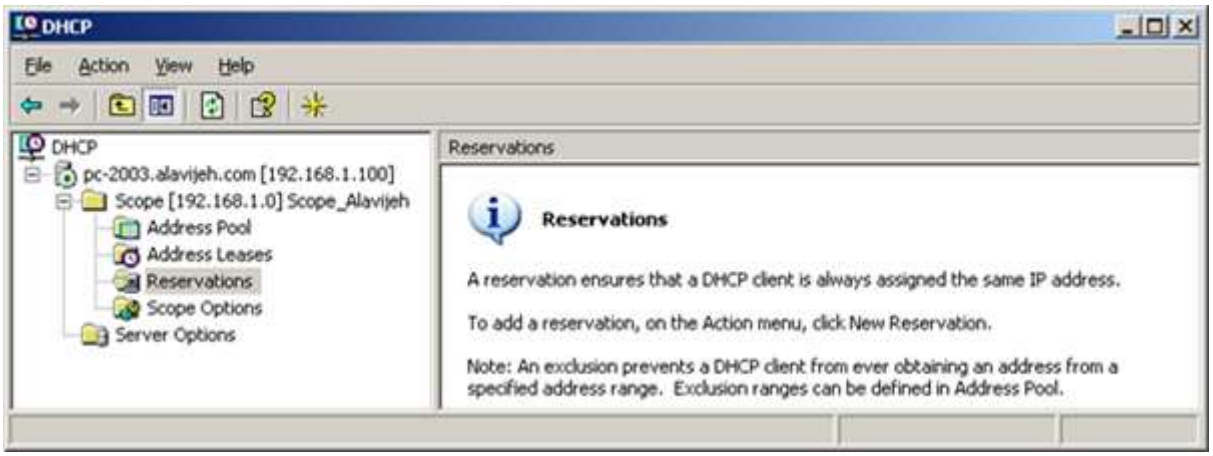
۱. **Address Pool (استخر آدرس)**: این قسمت بیانگر محدوده آدرس های قابل تخصیص و محدوده آدرس های غیر قابل تخصیص (Exclude) است.



۲. **Address Leases (آدرس های اجاره داده شده)**: بیانگر آدرس IPهایی می باشد که تا کنون به Clientها تخصیص داده شده است.



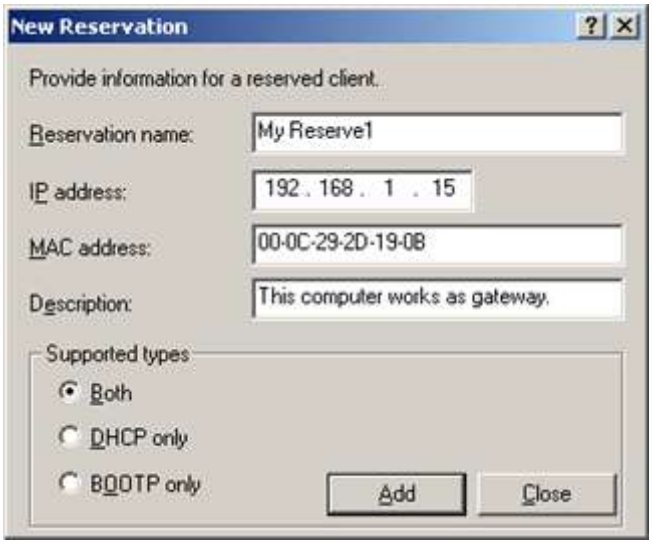
۳. **Reservation (رزرو شده ها)**: توسط این قسمت می توانید آدرس هایی خاص را همیشه به کامپیوتر هایی خاص نسبت بدهید. به عبارت دیگر زمانی که Clientی خاص درخواست IP بدهد، همیشه IPی ثابت و مشخص به وی تحویل داده خواهد شد.



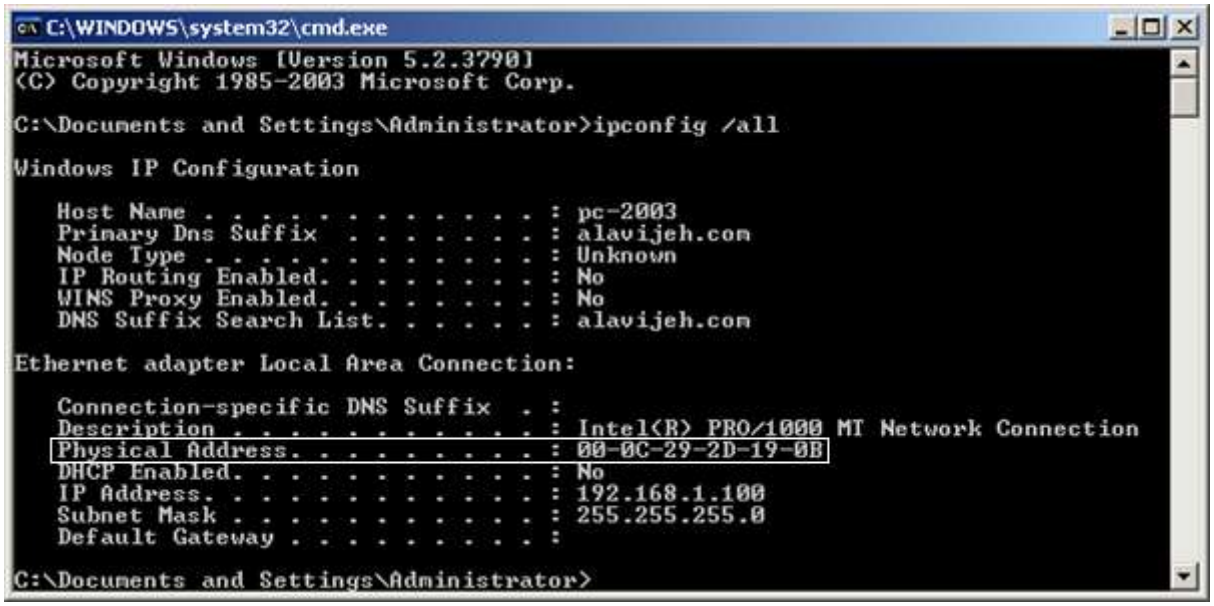
برای ایجاد IP رزرو شده جدید، روی گزینه Reservation راست کلیک کرده و گزینه New Reservation را انتخاب نمایید.

در صفحه باز شده، موارد زیر را وارد نمایید.

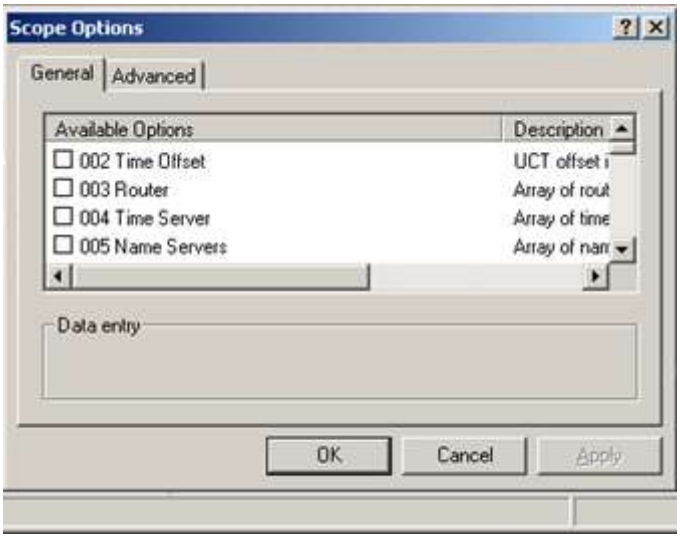
۱. Reservation Name : نامی دلخواه برای آدرس تخصیص داده شده
۲. IP Address : آدرس IP که می خواهید تخصیص دهید.
۳. MAC Address : بیانگر آدرس سخت افزاری کارت شبکه Client است که می خواهیم **همیشه** این آدرس IP را به آن اختصاص دهیم. برای به دست آوردن آدرس MAC یک کامپیوتر راه دور، می توان از دستور GetMac استفاده نمود.



برای یافتن آدرس MAC، در Client بدین صورت عمل کنید: در **Client** وارد محیط Command Prompt شده و دستور IpConfig /All را وارد نمایید. با این کار آدرس IP را در قسمت Physical Address مشاهده خواهید نمود. آن را در جعبه متن فوق، به همراه علامت ←، وارد نمایید.



۴. **Scope Option**: از طریق این قسمت می توانید تنظیمات تخصصی مربوط به DHCP Server را تعیین نمایید.



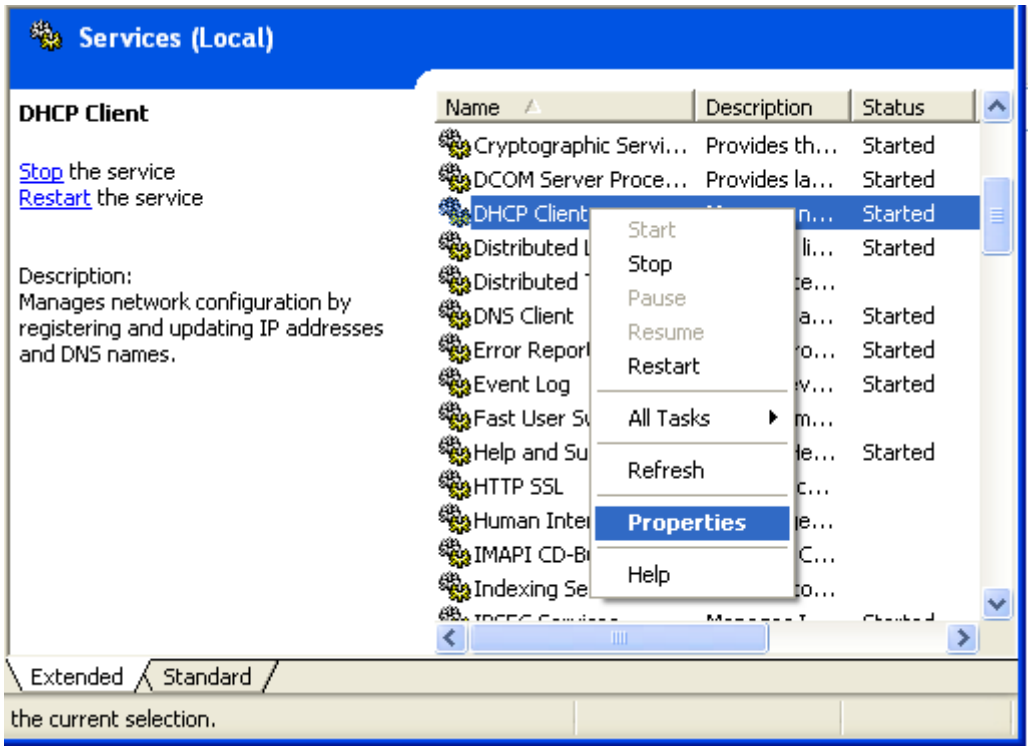
۲۰-۳-۲- تنظیم Client جهت استفاده از DHCP Server

از نظر تئوری با انجام موارد فوق، از این پس Clientها قادر به دریافت IP خود از سرور می باشند. (در صورتی که نحوه دریافت IP خود را روی Automatic تنظیم کرده باشند). اما همیشه در عمل این موضوع رخ نمی دهد و بایستی تنظیماتی را در Client انجام دهیم.

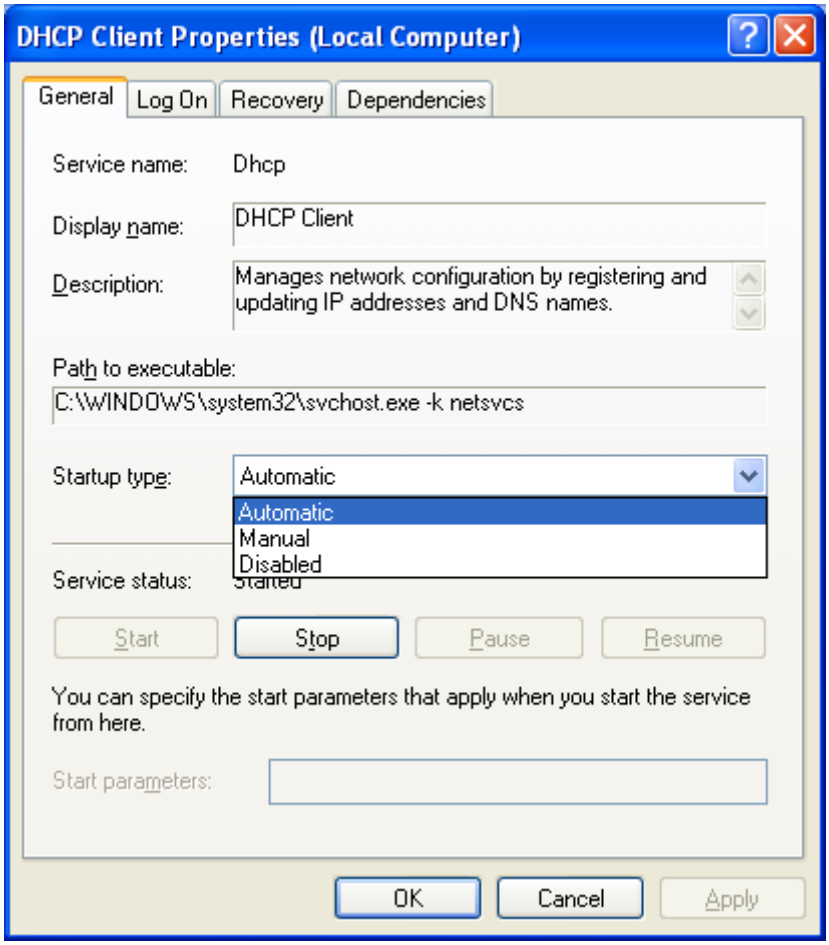
اولین گام فعال کردن DHCP Service (سرویس DHCP) است. برای این کار، در Client وارد مسیر زیر شوید:

Control Panel ➔ Administrative Tools ➔ Services

سپس روی گزینه DHCP Server راست کلیک کرده و گزینه Properties را انتخاب نمایید.



سپس در صفحه باز شده، از قسمت Startup type، گزینه Automatic را انتخاب کرده و OK کنید.

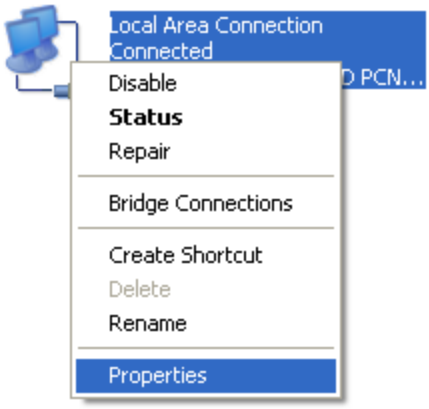


پس از OK کردن، توسط دکمه Start Service، سرویس DHCP Server را اجرا کنید. (البته ابتدا DHCP Server را انتخاب نمایید).

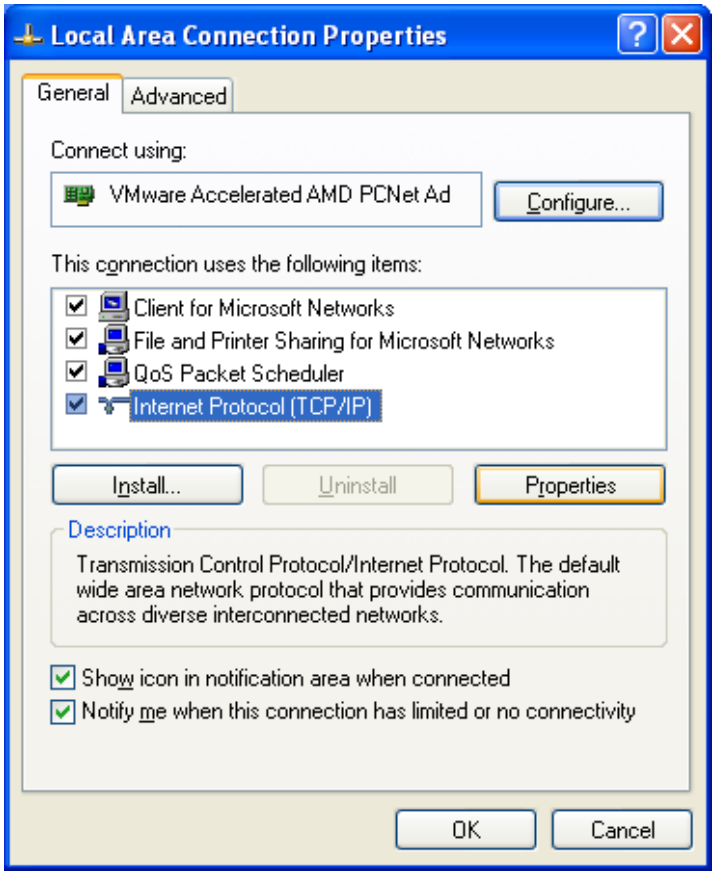
سپس در Client، وارد مسیر زیر شوید:

Control Panel ➔ Network Connections

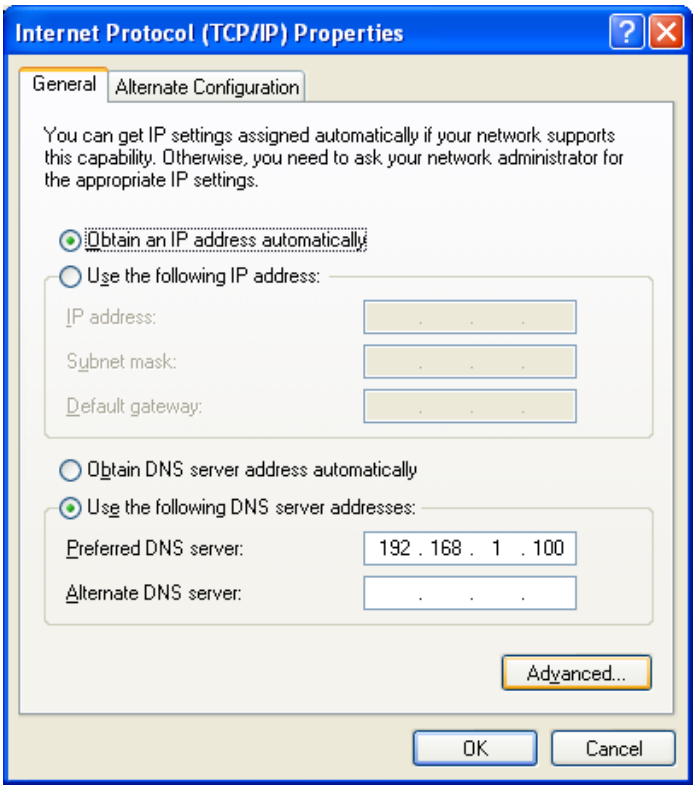
روی Local Area Connection راست کلیک کرده و گزینه Properties را انتخاب کنید.



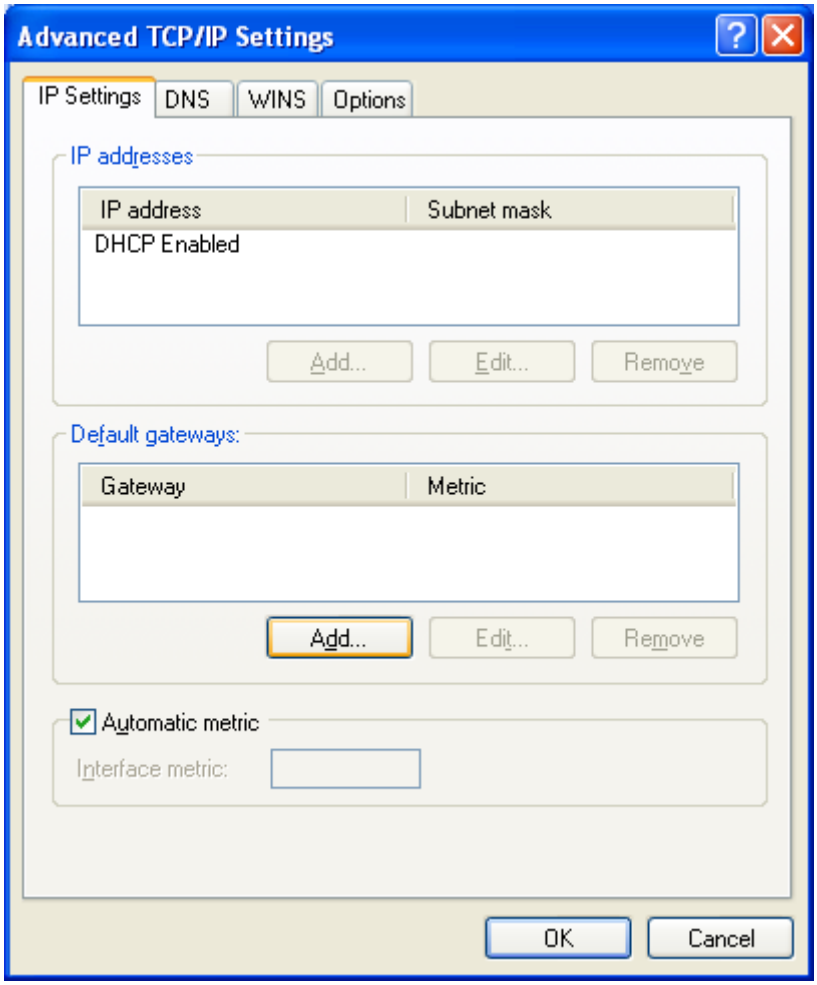
در صفحه باز شده، گزینه Internet Protocol (TCP/IP) را انتخاب کرده و روی دکمه Properties کلیک کنید.



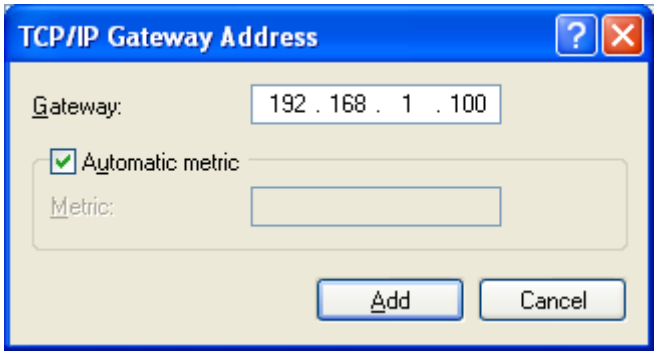
در صفحه باز شده، در قسمت بالا، گزینه Obtain an IP address automatically را انتخاب نماید. در قسمت پایین نیز گزینه Use the following DNS server addresses را انتخاب کرده و آدرس IP مربوط به DNS Server را وارد نمایید.



سپس روی دکمه Advanced کلیک کنید تا صفحه زیر باز شود. در این صفحه بایستی آدرس IP مربوط به DHCP Server را به عنوان Default Gateway انتخاب نمایید. به خاطر داشته باشید که Gateway، کامپیوتری بود که تمام بسته های خارج شده از کامپیوتر ما به سمت آن می رود. برای این کار در قسمت Default Gateway، روی دکمه Add کلیک کنید.



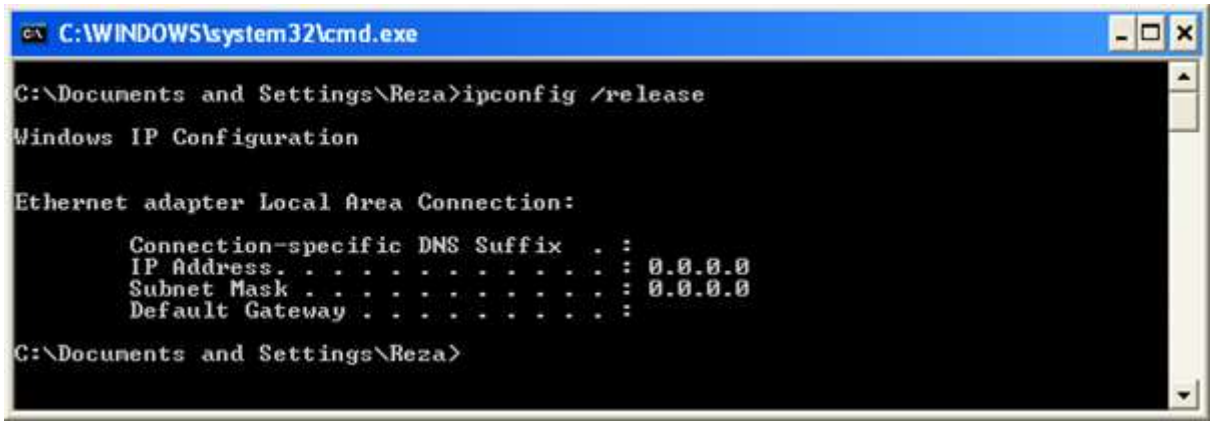
در صفحه باز شده، آدرس IP مربوط به DHCP Server را وارد نمایید.



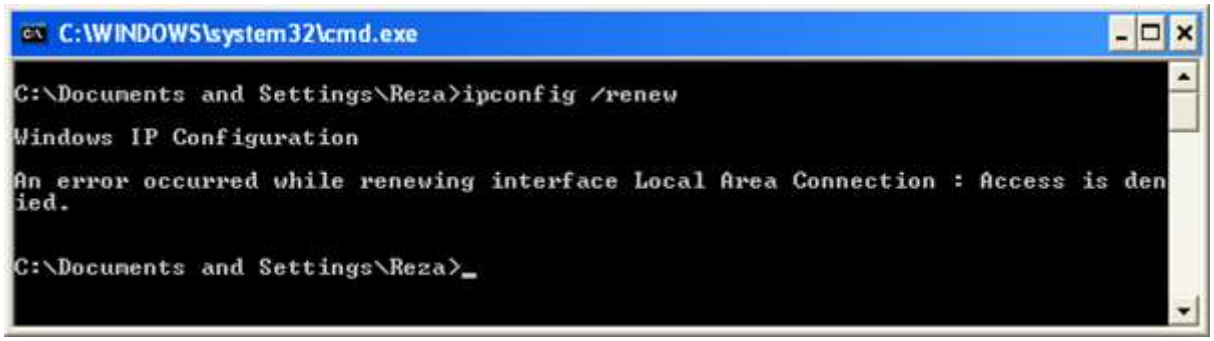
سپس روی Add کلیک کرده و OK بزنید تا تمام پنجره ها بسته شوند.

در گام بعدی بایستی آدرسی جدید از DHCP Server درخواست نمایید. لازمه این کار از بین بردن آدرس فعلی Client است.

برای این کار در محیط Command Prompt دستور IpConfig /release را وارد نمایید.

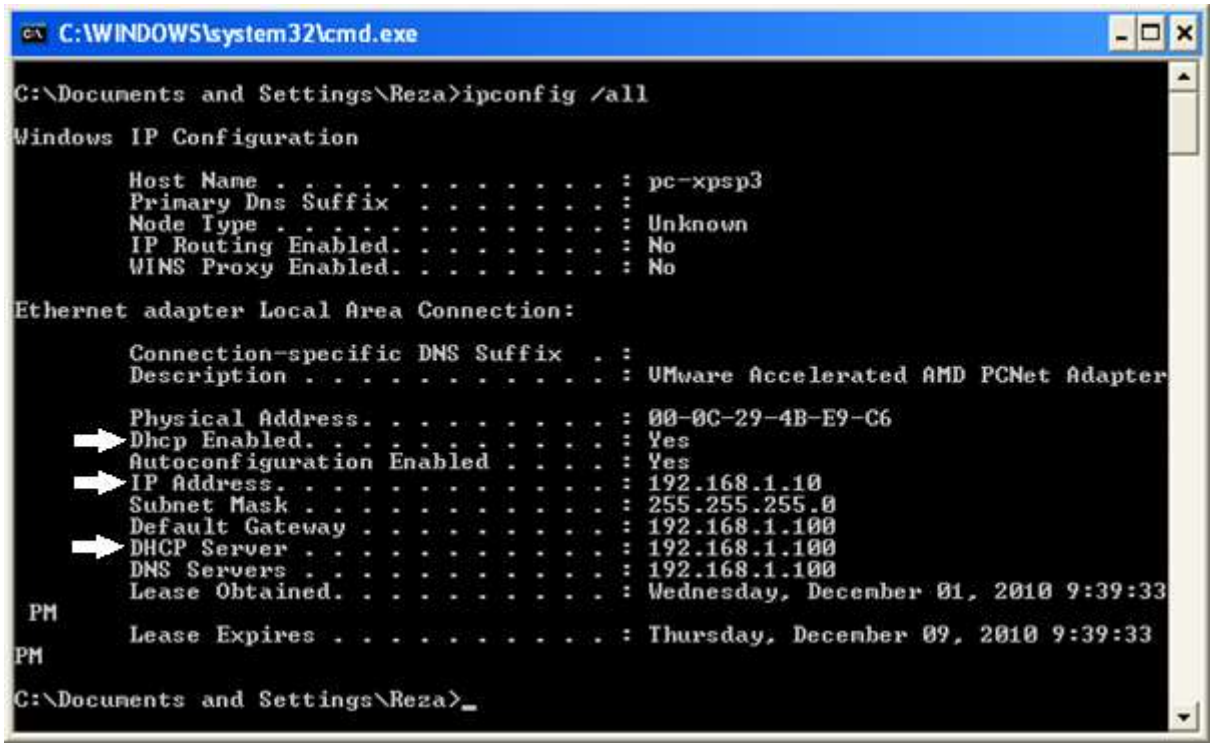


با این کار، دیگر Client آدرس IP ندارد. برای درخواست آدرس IP، دستور IpConfig /renew را وارد نمایید. با این کار، آدرس IP جدیدی از سمت Server به Client تخصیص داده می شود.

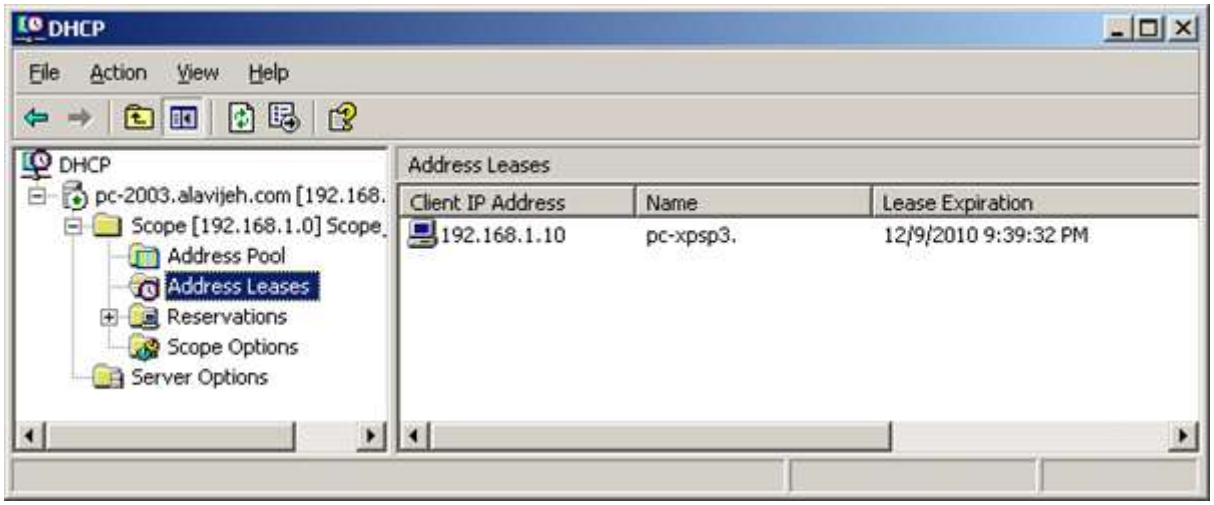


برای دیدن اطلاعات دقیق تر، در Client دستور IPConfig /All را وارد نمایید.

در شکل به قسمت DHCP Server و IP Address توجه فرمایید.

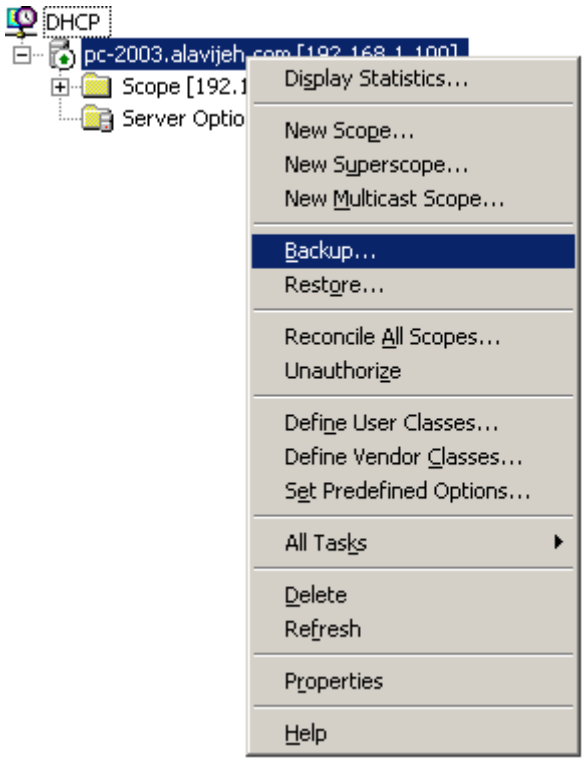


حال اگر مجددا به Server سری بزنید و وارد پنجره DHCP شوید، در قسمت Address Leases، مشاهده خواهید که Server به صورت خودکار، به Client یک آدرس IP تخصیص داده است.

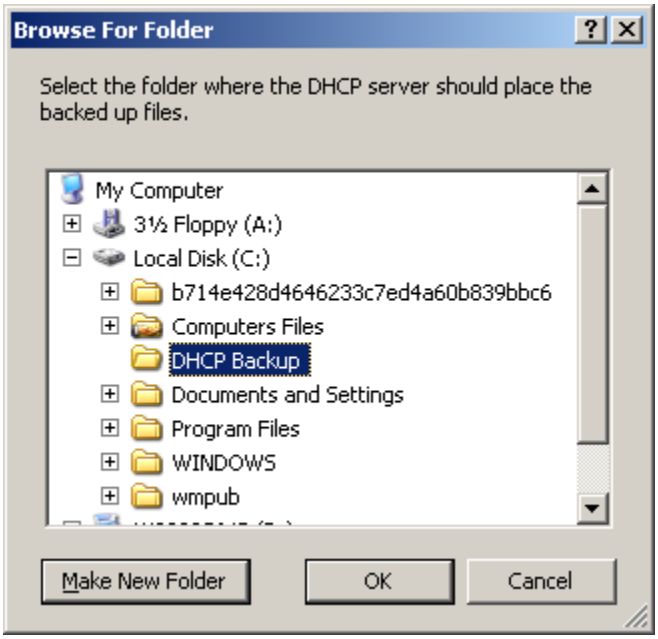


DHCP Backup & Restore -۴-۲۰

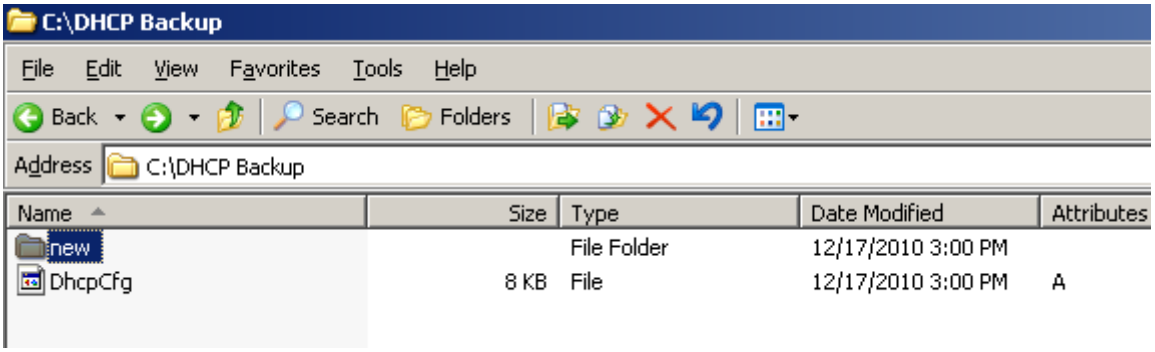
گاهی ممکن است به دلایل مختلفی بخواهید که سرویس DHCP موجود بر روی یک سرور را به سروری دیگر انتقال دهید. در این حالت بایستی ابتدا از اطلاعات مرتبط با سرویس DHCP در سرور اول پشتیبان تهیه نموده، سرویس DHCP را غیر فعال کرده و سپس فایل های پشتیبان تولید شده را به سرور دوم انتقال دهید. یا حتی ممکن است بخواهید یک کپی پشتیبان از DHCP خود داشته باشید (البته ویندوز خودش به صورت خودکار هر ۳۰ دقیقه یکبار از DHCP کپی پشتیبان می گیرد). بدین منظور ابتدا وارد DHCP ➔ Administrative Tools ➔ Start شده، روی سرویس DHCP راست کلیک کرده و گزینه Backup را انتخاب کنید.



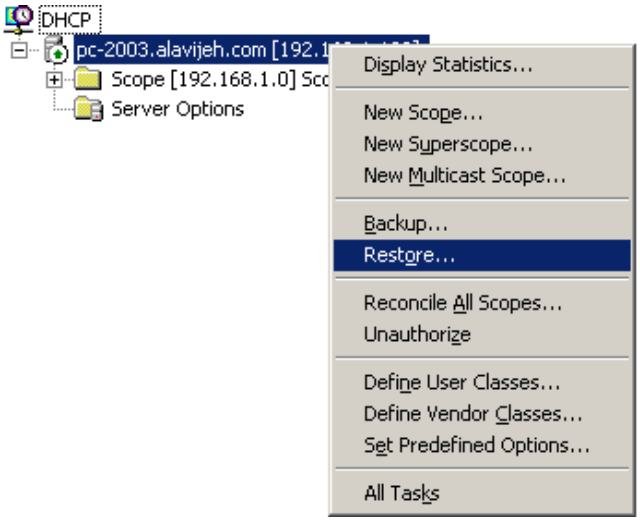
سپس در صفحه باز شده، مسیری را برای ذخیره فایل های کپی پشتیبان تعیین نمایید. در این مثال، آدرس مورد نظر C:\DHCP Backup است.



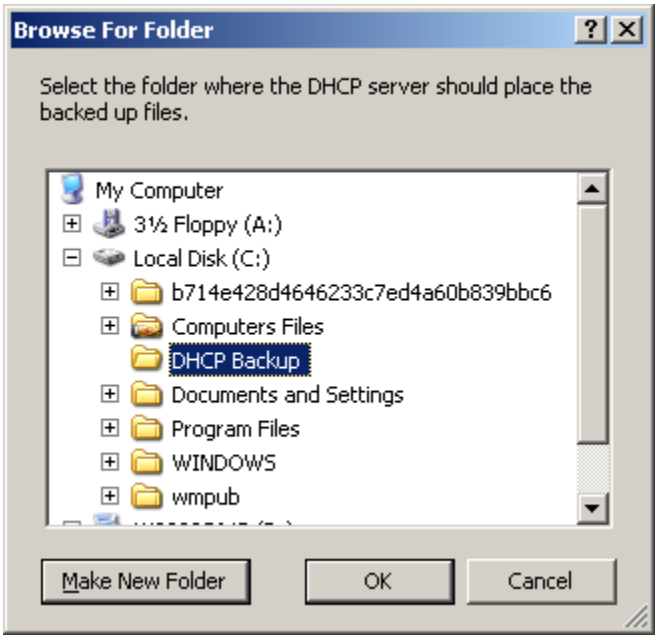
در اینصورت، سیستم در مسیر تعیین شده، فایل هایی را ایجاد خواهد نمود.



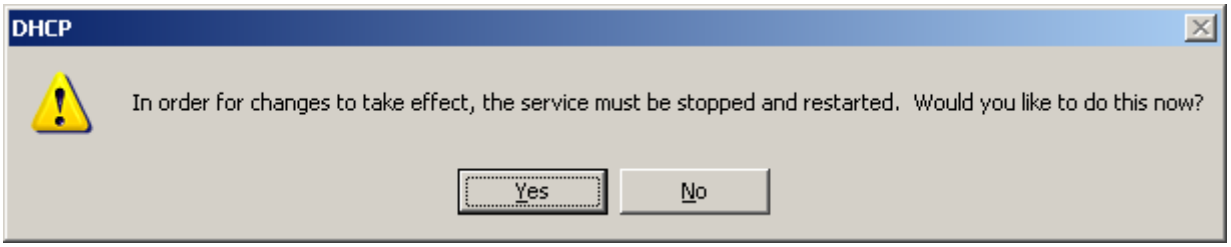
حال نوبت به باز گردانی (Restore) اطلاعات DHCP می شود. بدین منظور روی سرویس DHCP مورد نظر (در کامپیوتر خودتان یا در یک کامپیوتر دیگر) راست کلیک کرده و گزینه Restore را انتخاب کنید.



در صفحه باز شده، مسیری که فایلهای Backup در آن قرار دارد را انتخاب نمایید. در این مثال، این مسیر برابر با C:\DHCP Backup است.

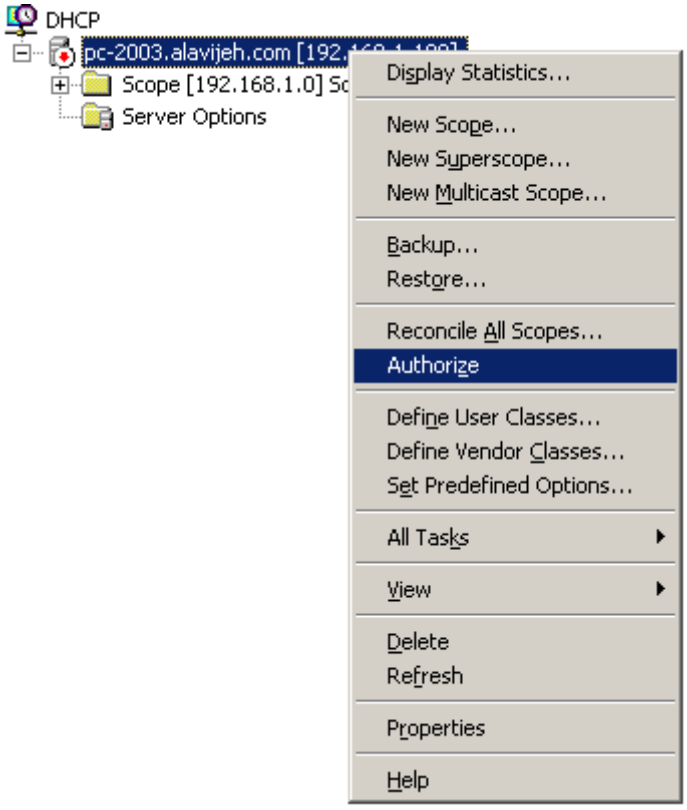


پس از انتخاب مسیر، سیستم می گوید که برای مشاهده تاثیرات Backup، بایستی سرویس DHCP، ابتدا Stop و مجددا Restart شود. روی OK کلیک کنید.



مدتی صبر نمایید تا تغییرات در شبکه اعمال شود.

بعد از اتمام عملیات باز گردانی اطلاعات، این بار نوبت به Authorize نمودن سرور DHCP می باشد. به منظور انجام این کار کافیست طبق تصویر زیر عمل کنید:



اگر عمل Restore را در سرور دیگری انجام دهید، حال اگر کلاینت های موجود در شبکه، راه اندازی مجدد (Restart) گردند، سرور دوم را به عنوان سرور DHCP خود بر می گزینند. فقط توجه داشته باشید که در این حالت بایستی DHCP اولیه را غیر فعال کنید.

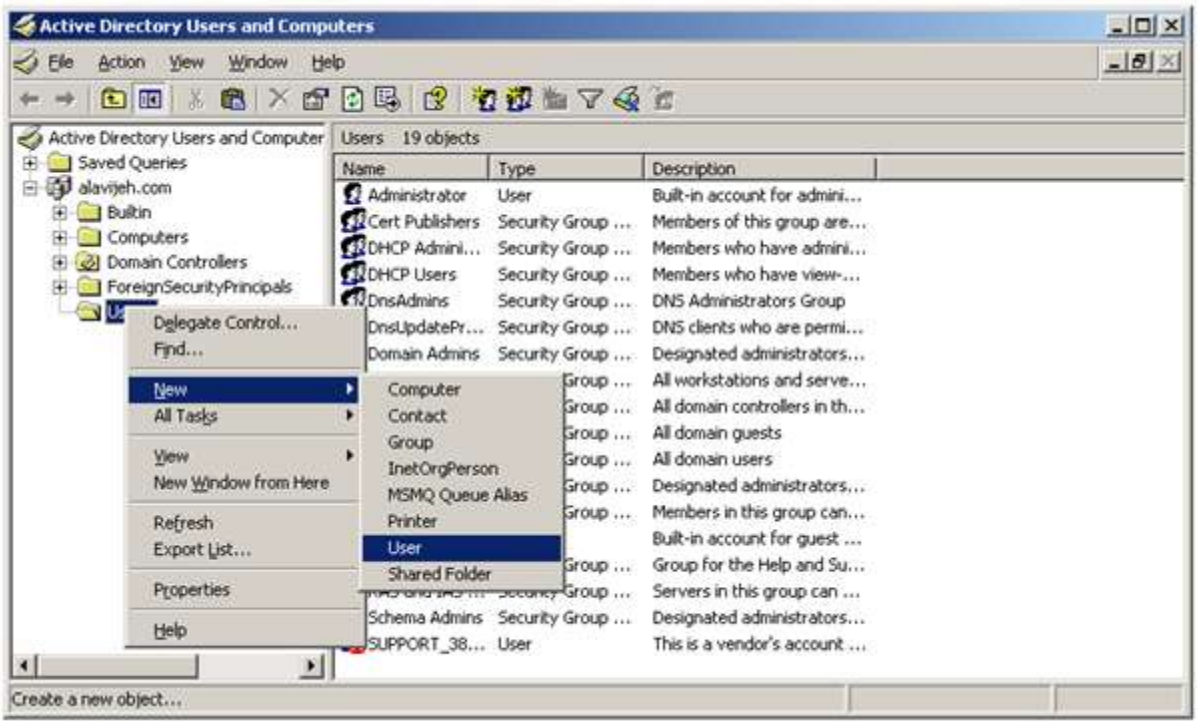
فصل ۲۱

اتصال Client به Domain

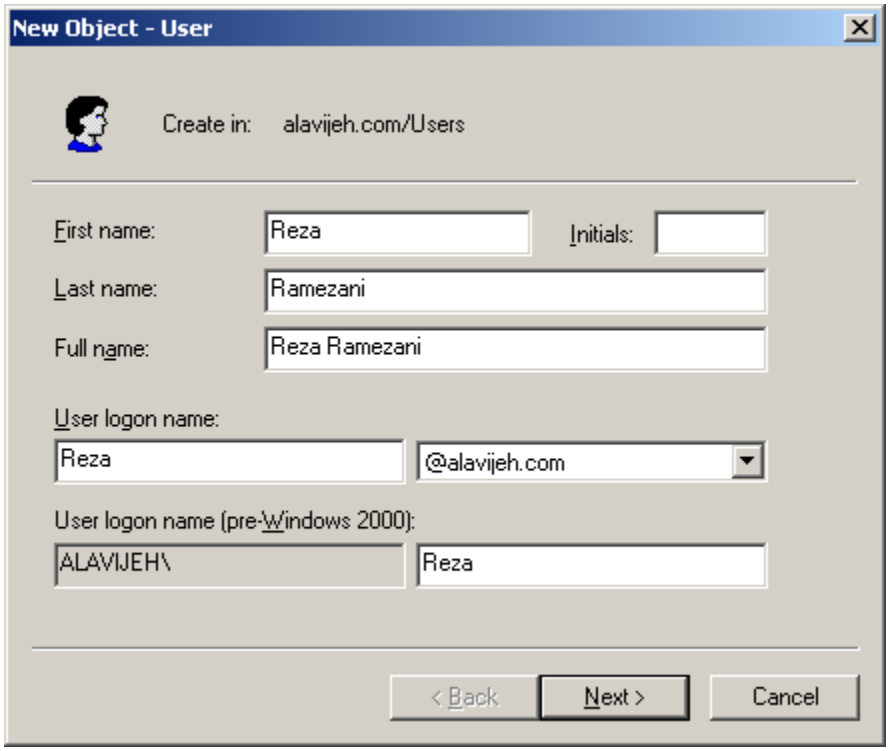
۲۱-۱- تنظیمات Server

پس از راه اندازی Server (نصب Active Directory)، نوبت به این کار می رسد که Client ها را به Server متصل کرده و آن را عضوی از Domain کنیم. بدین منظور ابتدا یک نام کاربری و رمز عبور برای Client و در Server تعریف کنید تا بـه کمـک آن Client بتواند به سرور Login کرده و به آن متصل شود. برای این کار، در سرور از منـوی Start، گزینـه Administrative Tools و سپس گزینه Active Directory Users and Computers را انتخاب نمایید.

سپس در صفحه باز شده، قسمتی که نام دامنه را نشان می دهد، بسط داده، روی قسمت Users راست کلیک کـرده و سـپس User ➔ New را انتخاب نمایید.



سپس در قسمت بالا، نام و نام خانوادگی کاربر را وارد نمایید. سپس در قسمت User logon name، نام کاربری کاربر که هنگام ورود به سیستم باید وارد کند را در این قسمت وارد نمایید. سپس روی Next کلیک کنید.



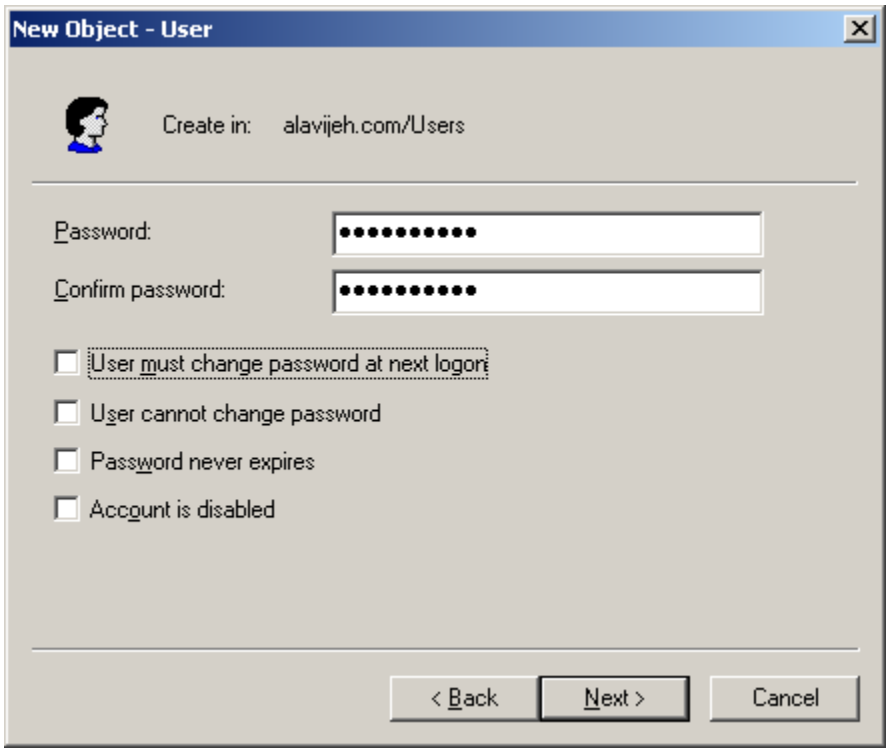
سپس در این صفحه، رمز عبور کاربر را وارد نمایید. توجه نمایید که در ابتدا به صورت پیش فرض، در ویندوز سرور، رمز عبور بایستی دارای حداقل ۷ حرف بوده و نیز به صورت Complex (پیچیده) باشد (این تنظیمات در Group Policy تعیین می گردد که در فصل های بعدی توضیح می دهیم). در این مثال ما رمز عبور را abc@abc123 وارد کردیم. در زیر ۴ گزینه وجود دارد که به توضیح مختصر آن می پردازیم:

۱. **User must change password at next logon:** با فعال کردن این گزینه، سیستم کاربر را مجبور می کند که هنگام **اولین** Login به سیستم، رمز عبور خود را تغییر دهید. **توجه:** اگر بخواهید سیستمی را به Domain خود Join کنید و هنگام Join کردن از این نام کاربری استفاده کنید؛ و همچنین اگر تاکنون با این کاربر Login نکرده اید و این گزینه را نیز فعال کرده باشید، سیستم اجازه ورود شما را خواهد گرفت.

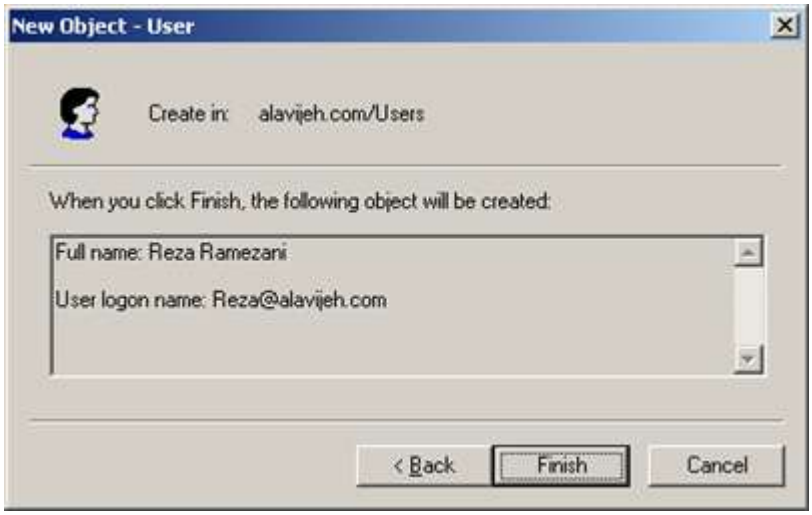
۲. **User cannot change password:** با فعال کردن این گزینه، کاربر قادر به تغییر دادن رمز عبور خود نخواهد بود. بهتر است این گزینه را غیر فعال کنید.

۳. **Password never expires:** با فعال کردن این گزینه، رمز عبور کاربر هیچ گاه منقضی (Expire) نخواهد شد. در غیر اینصورت به صورت پیش فرض، پس از ۴۲ روز، کاربر مجبور به تغییر رمز عبور خود است. علت این امر بالا بردن امنیت رمز عبور است.

۴. **Account is disabled:** با فعال کردن این گزینه، کاربر غیرفعال شده و قابلیت ورود به سیستم را از دست خواهد داد.



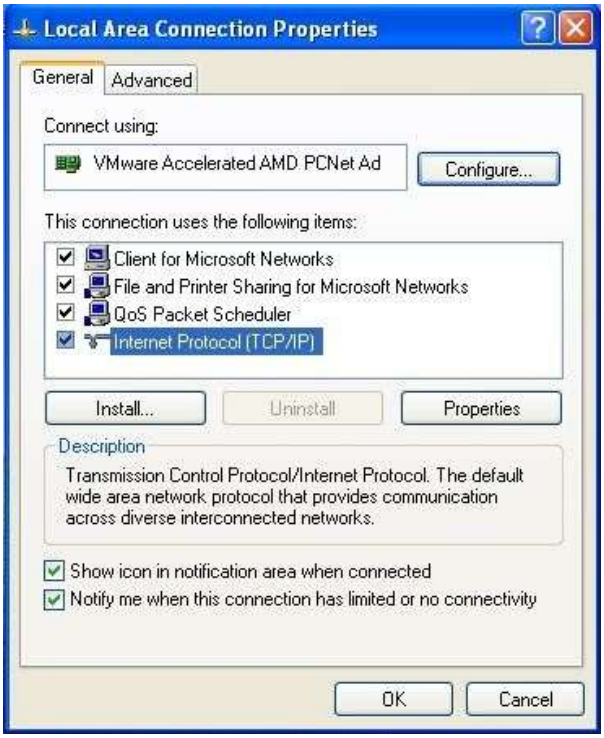
در مرحله آخر، اطلاعات مختصری در مورد کاربر را مشاهده خواهید نمود. برای ساخت کاربر، روی دکمه Finish کلیک نمایید.



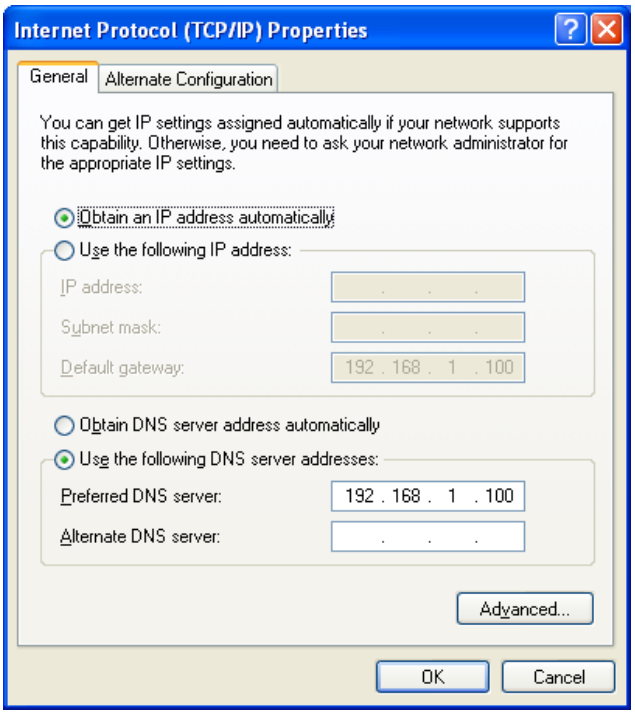
۲۱-۲- تنظیمات Client

پس از تعریف نام کاربری و رمز عبور در Server، نوبت به انجام تنظیماتی در Client می شود. برای شروع ابتدا از متصل بودن Client مطلع شوید. بدین منظور در Client در Network Connection ➔ Control Panel روی Local Area Connection، دو بار کلیک کنید. در صورت اتصال Client به شبکه، بایستی صفحه ای مانند صفحه زیر مشاهده کنید. سپس باید تنظیمات IP Address و DNS Address مربوط به Client را انجام دهید. برای این کار روی دکمه Properties کلیک کنید.

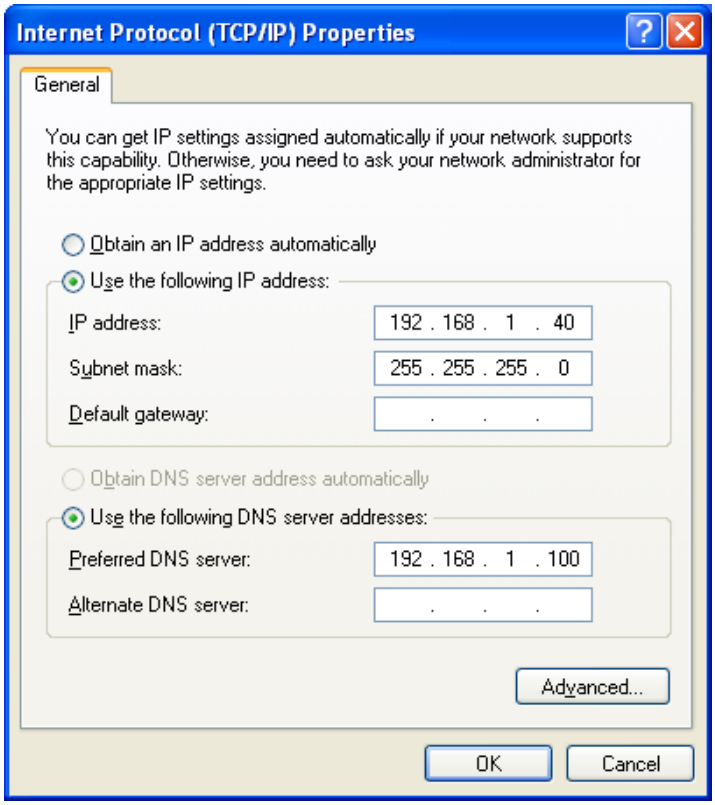
برای تنظیم کردن IP، ابتدا گزینه Internet Protocol (TCP/IP) را انتخاب کرده و سپس روی دکمه Properties کلیک کنید.



حال نوبت به تنظیم آدرس IP در Client می شود. در این مرحله، اگر در شبکه خود از DHCP Server استفاده می کنید، بایستی صفحه را به صورت زیر تنظیم نمایید (برای اطلاعات بیشتر به فصل DHCP و قسمت اتصال Client مراجعه نمایید). تنها نکته مهم این است که در قسمت Preferred DNS Server، بایستی حتما آدرس DNS Server را وارد نمایید. البته **توجه** فرمایید که اگر DHCP Server آدرس DNS Server را نیز بدهد، نیازی به پر کردن این قسمت نیست (آیا به خاطر دارید که هنگام ایجاد Scope جدید در DNS Server، می توانستیم آدرس DNS Server را نیز تعیین نماییم؟).

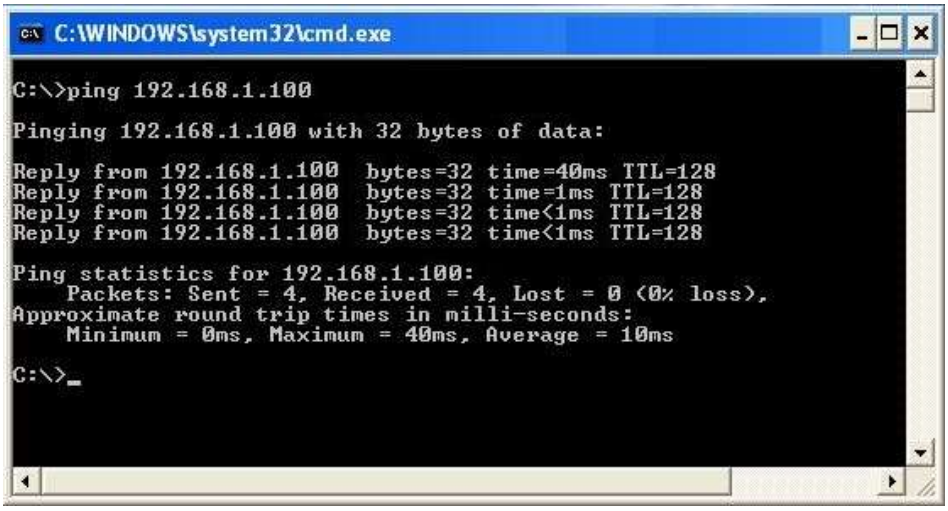


اما اگر قصد دارید IP Address مربوط به Client را به صورت دستی تنظیم کنید، بایستی آن را به گونه ای وارد کنید کـه بـه صورت منطقی در شبکه سرور (Domain Controller) قرار گیرد. یعنی آدرس های IP کلاینـت و سـرور بایـد قسـمت شـبکه اشان با هم برابر باشد (یعنی قسمت Network Address آن ها با هم برابر باشد). مـثلاً دو آدرس آی پـی ۱۹۲.۱۶۸.۱.۱۰۰ و ۱۹۲.۱۶۸.۱.۴۰ هر دو از نظر منطقی در یک شبکه قرار دارند. همچنین حتما باید در قسمت Preferred DNS Server، آدرس سروری که DNS روی آن نصب شده است را وارد نمایید. توجه نمایید که اگر این قسمت را بـه درسـتی وارد نکنیـد، Client قابلیت اتصال به Domain را پیدا نخواهد کرد.

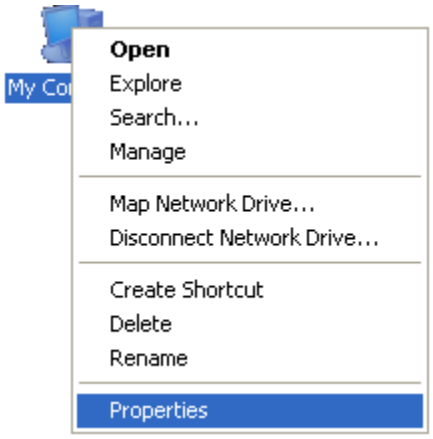


برای تست ارتباط شبکه کافیست همانند تصویر زیر، با استفاده از دستور Ping از صحت ارتبـاط کلاینـت بـا سـرور، اطمینـان حاصل نماییم. بدین منظور دستور زیر را وارد نمایید:

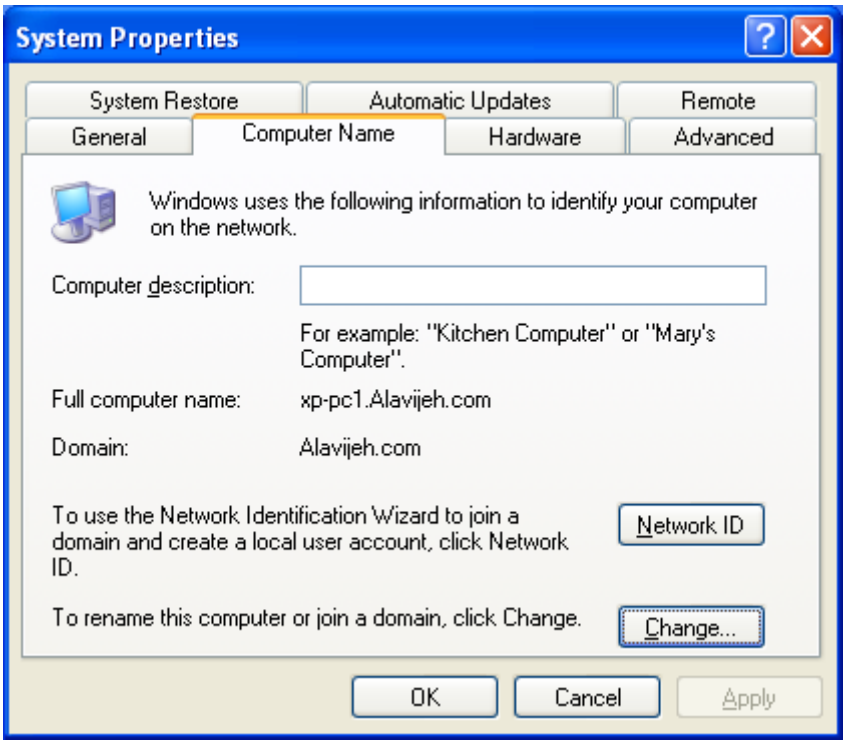
C:\> **Ping** آدرس/نام سرور



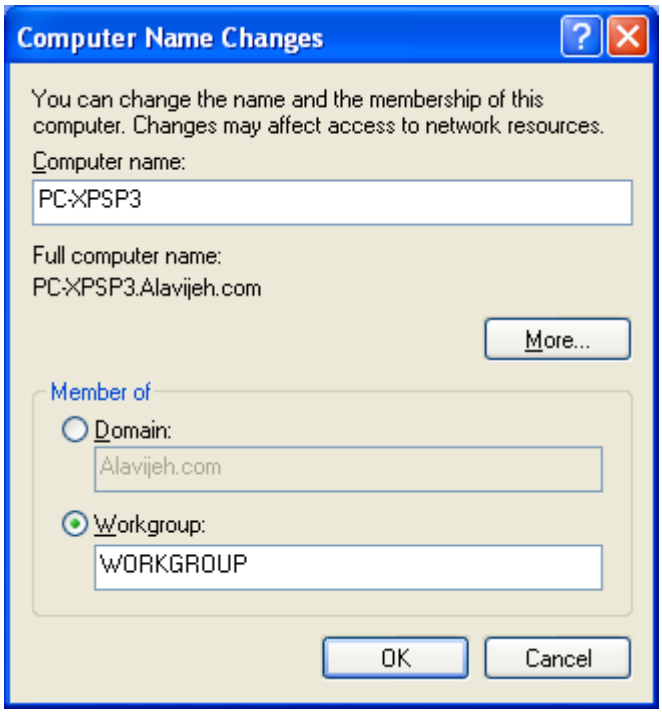
پس از اطمینان از صحت قابلیت اتصال Client به Server، بایستی تنظیمات نهایی Client را انجام دهید تا Client عضوی از دامنه شود. برای این کار روی My Computer راست کلیک کرده و گزینه Properties را انتخاب کنید.



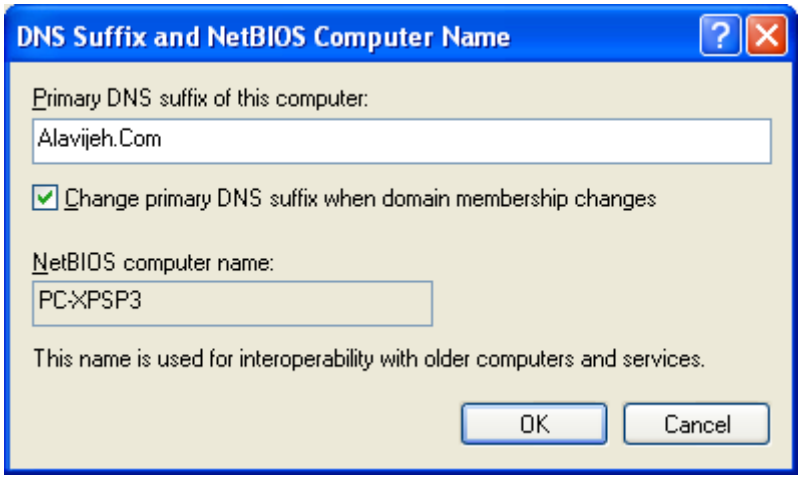
سپس سربرگ Computer Name را انتخاب کرده و سپس روی دکمه Change کلیک کنید.



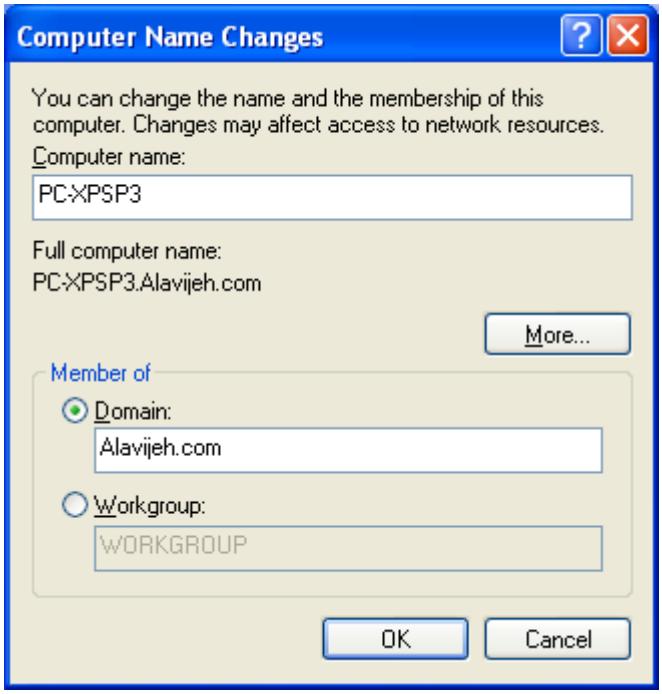
سپس در صفحه باز شده، مشاهده خواهید کرد که کامپیوتر شما عضوی از Workgroup است.



سپس روی دکمه More کلیک کرده و نام Domain Controller را وارد نمایید.



سپس روی دکمه OK کلیک کنید. سپس در صفحه باز شده، گزینه Domain را انتخاب کرده و سپس در جعبه متن مربوطه، نام کامل Domain Controller را وارد نمایید.



بعد از کلیک کردن روی دکمه OK، بایستی نام کاربری و رمز عبوری را که در سرور ثبت کرده اید را در پنجره باز شـده وارد نمایید.

بعد از OK کردن، اگر نام کاربری و رمز عبور درست باشد، سیستم به شما پیغام خوش آمد گویی به دامنه را می دهد.

با دیدن پنجره فوق اطمینان حاصل می نماییم که کار به اتمام رسیده است. سپس باید Client را Restart کنید:

پس از Restart شدن Client، صفحه ای مانند صفحه زیر وارد می شود.

باز فشردن کلیدهای Ctrl + Alt + Delete، صفحه ای مانند صفحه زیر باز می شود. از طریق این صـفحه مـی توانیـد ۲ روش برای ورود به سیستم انتخاب کنید:

۱. **This Computer**: که برای این کار بایستی نام کاربری و رمز عبوری را وارد نمایید که بـر روی همـین Client ثبـت شده است. (مانند روش قبل)
۲. **To Domain**: در این روش بایستی نام کاربری و رمز عبوری را وارد نمایید که بر روی Server تعریف شده باشـد. در این صورت شما فقط کارهایی را بر روی سیستم می توانید انجام دهید که مدیر شبکه اجازه انجام آن کارها را به شما داده باشد.


Log On to Windows
Microsoft
Windows xp
Professional
Copyright © 1985-2001
Microsoft Corporation
Microsoft
User name:
Reza
Password:
Log on to:
ALAVIJEH
ALAVIJEH
PC-XPSP2 (this computer)
OK
Cancel
Shut Down...
Options <<

فصل ۲۲

Active Directory Users And Computers

۲۲-۱- آشنایی با انواع Account ها و ابزارهای مدیریتی

در Active Directory، Account ها به ۳ دسته تقسیم می شوند:

۱. **User Account:** به ازاء هر کاربر در Domain یک User Account باید ایجاد کنید. از این نوع Account ها برای Log On کردن به Domain و دسترسی به منابع آن استفاده می شود.

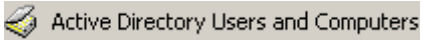
۲. **Computer Account:** به ازاء هر کلاینت، هر سرور و هر DC که عضو Domain هست یک Computer Account وجود دارد و در آنها برای اعمال کردن Policy ها از Authentication استفاده می شود.

۳. **Group Account:** برای مدیریت راحت کاربران (عضویت افراد در گروه ها) و اعطای مجوز به آنها و همچنین اعمال Policy از این نوع Account ها استفاده می شود.

۲۲-۲- مدیریت در Active Directory user and computer

برای مدیریت و اجرای این بخش مسیر زیر را دنبال میکنیم.

Start➔Administrative Tools➔ Active Directory Users and Computers



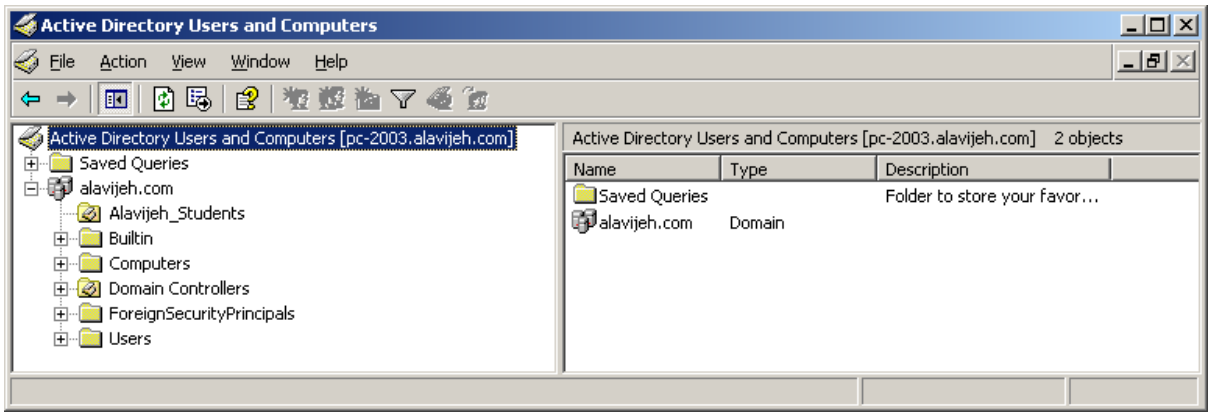
پس از اجرا، پنجره Active Directory Users and Computers اجرا می شود که به شکل زیر است:

همچنین قابل ذکر است که:

تمامی کاربران و گروه های که در Domain ایجاد می شوند، داخل پوشه Users قرار می گیرند.

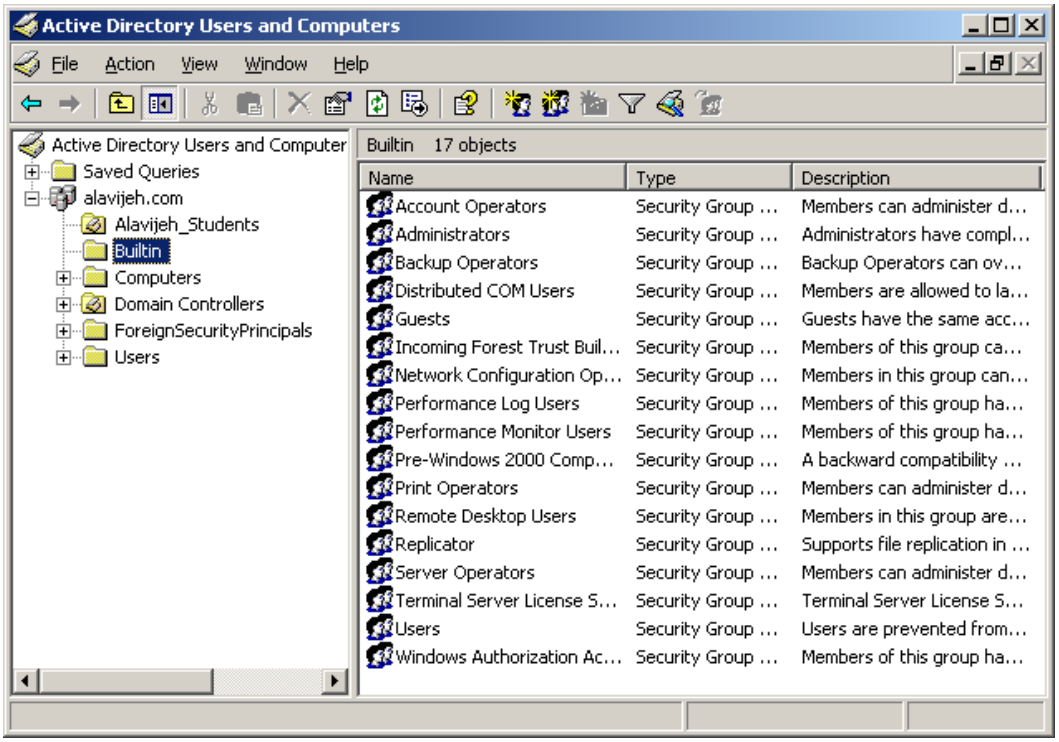
به ازاء تمامی کامپیوتر هایی که عضو Domain می شوند، یک Computer Account در پوشه Computers ایجاد می شود.

تمامی گروه هایی که به صورت پیش فرض ایجاد می شوند، در پوشه Builtin قرار می گیرند.



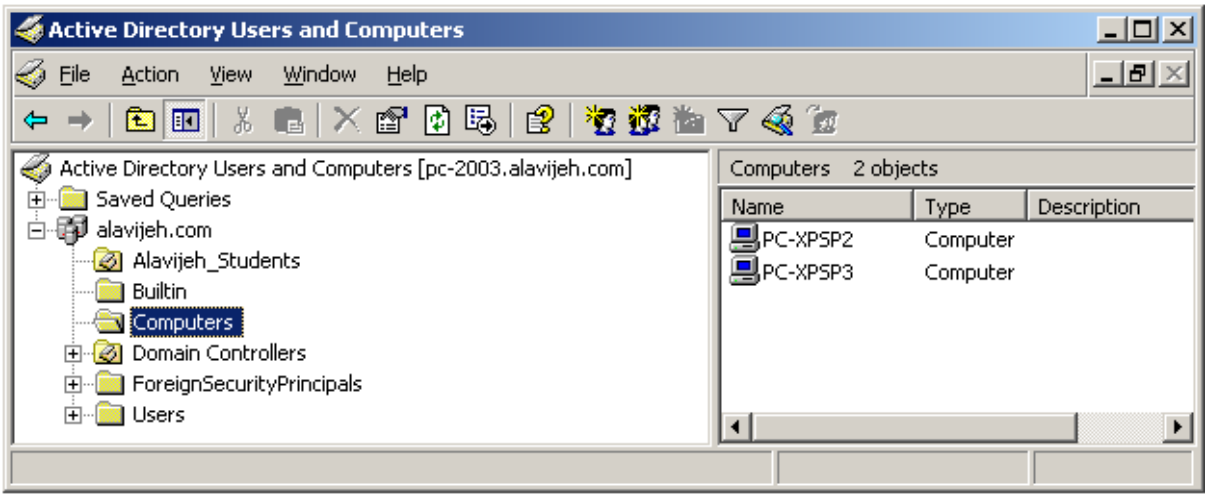
۲۲-۲-۱- آشنایی با گروه های Builtin

گروه های Builtin، گروه هایی هستند که زمان نصب Active Directory به صورت پیش فرض همراه با برنامه نصب و ایجاد می شوند و می توان آنها را در پوشه های Builtin و Users مشاهده کرد.



۲۲-۲-۲- پوشه Computers

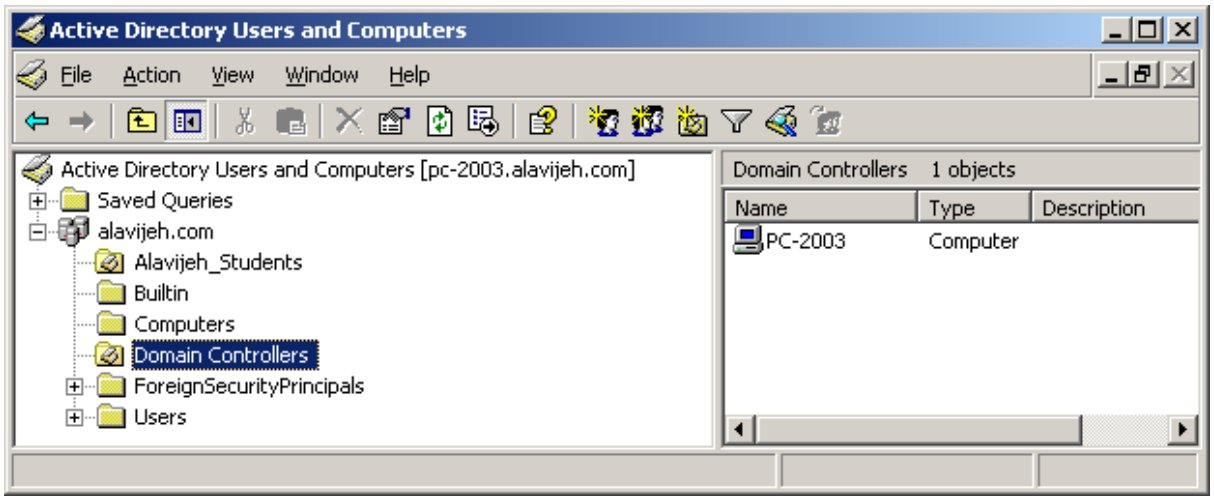
به ازاء تمامی کامپیوتر هایی که عضو یک Doman می شوند، یک Computer Account در پوشه Computers مانند شکل زیر ایجاد می شود.



۲۲-۲-۳-

۲۲-۲-۴- *Domain Controllers*

هر کامپیوتری که عضو Domain می شود، به صورت خودکار برای آن کامپیوتر یک Computer Account در پوشه Computers در داخل Domain ایجاد می شود. اما برای کامپیوتر هایی که DC باشند، یک Account در Domain Controllers ایجاد می شود. در شکل زیر، ما فقط یک Domain Controller داریم.



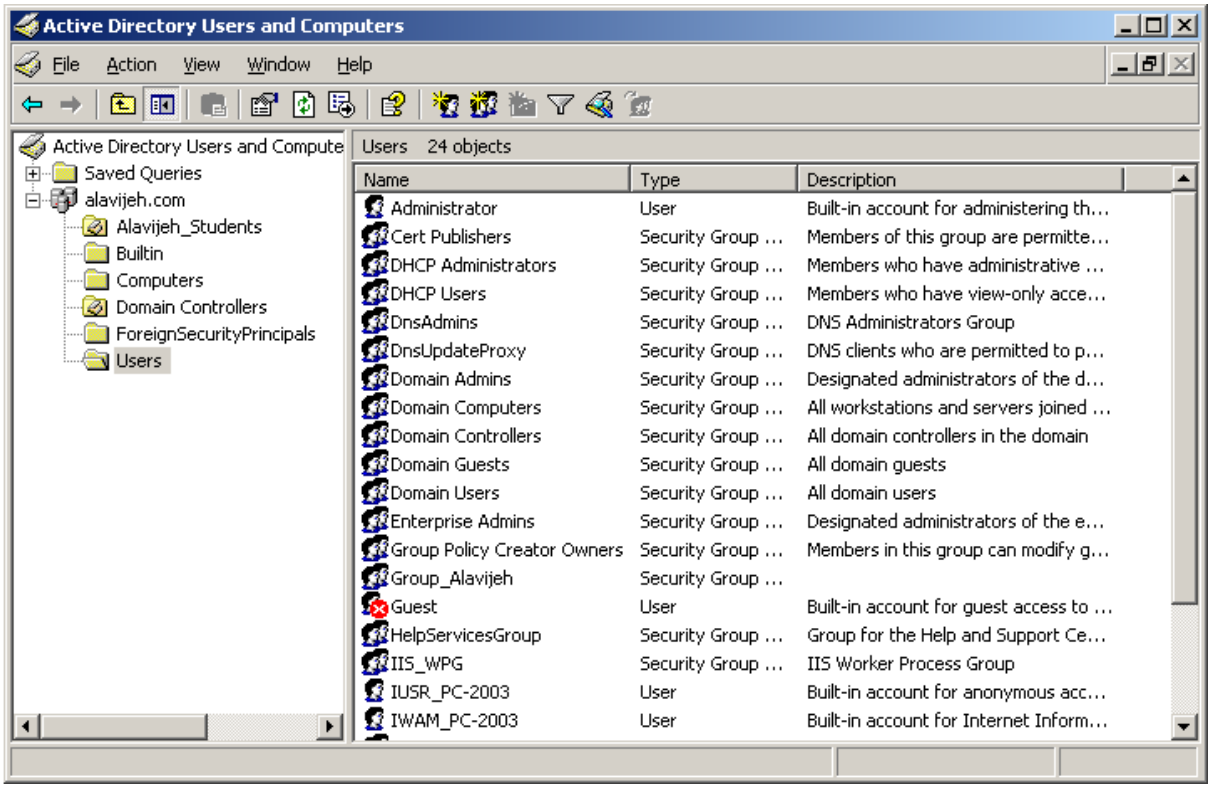
۲۲-۲-۵- *ForeignSecurityPrincipals*

یک نگهدارنده است که تایید کننده های امنیتی و هویتی را نگهداری می کند که این تایید کننده های امنیتی و هویتی با Objectها و عناصر دامنه های خارجی Trust (روابط اعتمادی) شده، مجتمع شده اند.

۲۲-۳- مدیریت کاربران و گروه ها

بخش Users یکی از مهمترین و اصلی ترین بخش های Active Directory Users and Computers است.

نظارت، مدیریت و کنترل کاربران در هر سازمانی مهمترین بخش است و این مدیریت در اینجا توسط قسمت Users انجام می شود. با انتخاب قسمت Users، لیست تمامی کاربران و گروه های سیستم را مشاهده خواهید نمود. تصویر بیانگر یک کاربر و تصویر بیانگر یک گروه است. وجود یک علامت ضربدر قرمز رنگ نیز (مانند) بیانگر غیرفعال بودن یک کاربر یا یک گروه می باشد.



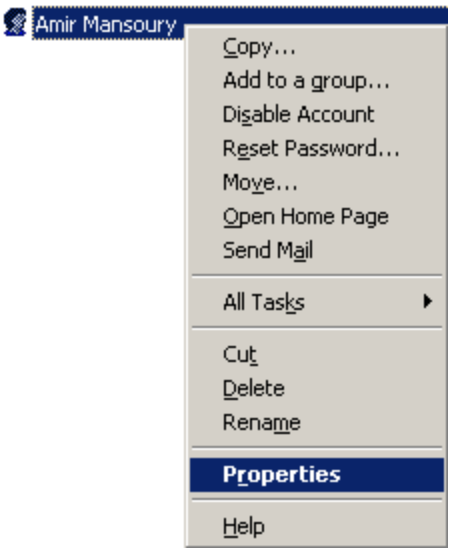
۲۲-۳-۱- تعریف کاربر، گروه و واحد سازمانی جدید

برای آشنایی با چگونگی تعریف کاربر، گروه یا واحد سازمانی جدید، به فصل User, Group, Organizational Unit مراجعه فرمایید.

۲۲-۴- مدیریت و تنظیمات کاربری

پس از ایجاد کاربر، مهمترین بخش آن مدیریت و تنظیمات کاربر جدید و دیگر کاربران می باشد. برای مدیریت کاربران به ترتیب مراحل زیر را دنبال میکنیم.

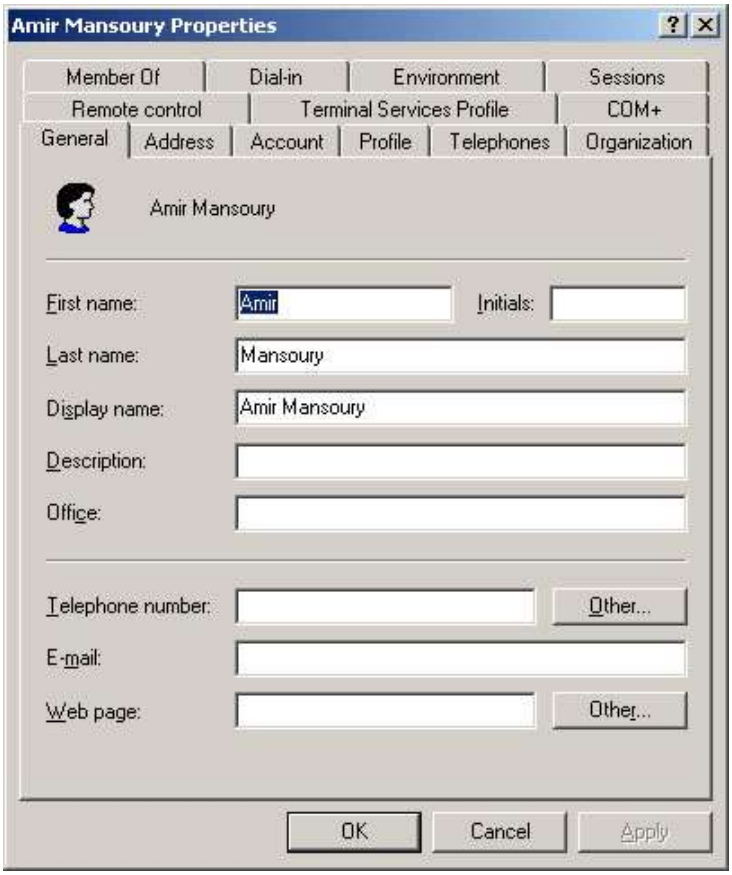
از پوشه User بر روی کاربر مورد نظر کلیک راست کرده و سپس گزینه Properties انتخاب کنید.



با این کار، پنجره زیر نمایان می شود. در این بخش هر Tab مرتبط با یکسری تنظیمات است که به صورت جدا به آنها میپردازیم.

۲۲-۴-۱- General

این بخش شامل اطلاعات کاربر بطور کلی میباشد که شامل نام، نام خانوادگی، اسم نمایش داده شده، توضیحات، آدرس ایمیل و.... میباشد.



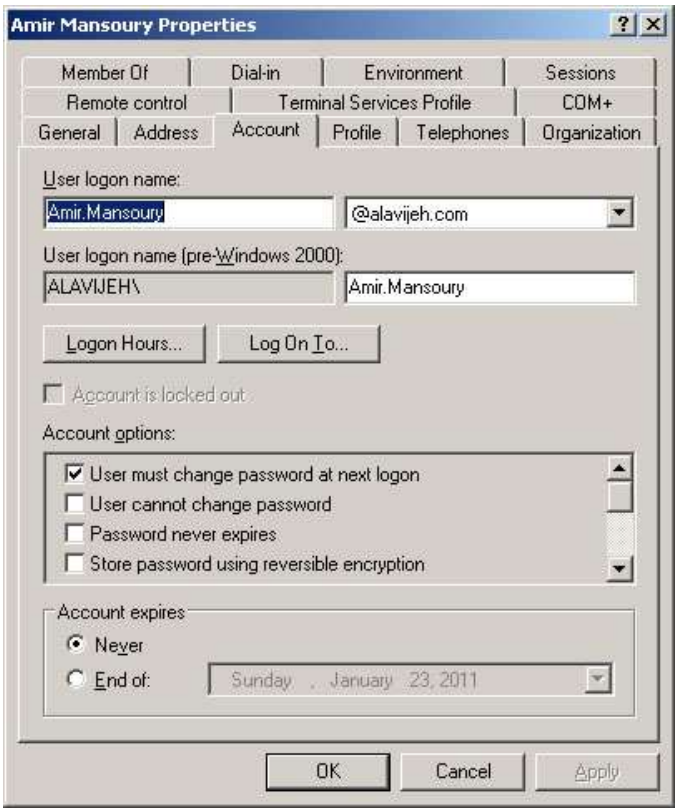
Account – ۲-۴-۲۲

در این بخش تنظیمات زیر قابل انجام است:

بخش User Logon Name که همان نام کاربری است.

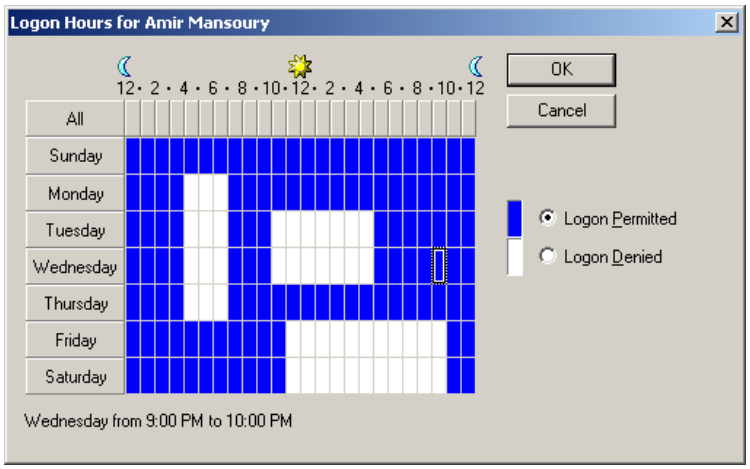
بخش Account Expires که توسط این گزینه می توانید برای کاربر محدودیت زمانی ایجاد کنید. بدین منظور که کاربر بعد از تاریخی خاص منقضی (Expire) شده و دیگر توانایی Login کردن را نداشته باشد. در ویندوز سرور بطور پیش فرض این گزینه بر روی Never تنظیم شده است. در صورت نیاز، می توانید زمان Expire شدن را تنظیم نمایید.

اما یکی از مهمترین مبحث ها در سیستم های کاربری، ساعت ورود و خروج کاربران به سیستم می باشد. شما به عنوان مدیر یک مجموعه باید بتوانید برای کاربران، ساعت های معینی را مشخص کنید تا کاربران فقط در این زمان ها بتوانند به سیستم وارد شوند. برای این کار از Login Hours استفاده میکنیم.



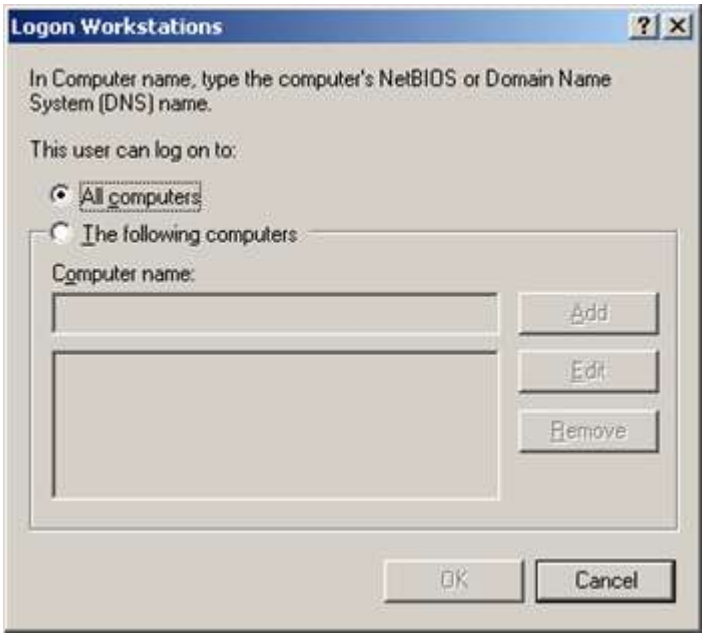
۲۲-۴-۳- Logon Hours برای کاربران

اگر روی دکمه Logon Hours کلیک کنید، شکلی مطابق شکل زیر به نمایش در می آید. این پنجره به شما نشان می دهد که کاربر در چه ساعات و در چه روزهایی، می تواند اجازه Login کردن به Domain را داشته باشد. شما می توانید هر کاربر را دارای محدودیتی زمانی در یکی از روزهای هفته و طی ساعاتی خاص بکنید. خانه هایی که با رنگ آبی پرشده اند بیانگر این موضوع هستند که کاربر در این ساعات و در این روزها اجازه Login کردن به Domain را دارد. شما می توانید با انتخاب یک خانه یا Select کردن خانه های متفاوت و گوناگون برای کاربر محدودیت ایجاد کنید. لذا باید آن خانه ها را به رنگ سفید در بیاورید که نشان دهنده آن است که کاربر در آن ساعات و در آن روزها اجازه Login به Domain را ندارد. بدین منظور بعد از انتخاب زمان های مورد نظر، روی قسمت Logon Denied کلیک کنید. البته باید توجه داشت که در ویندوز سرور، پیش فرض تمامی خانه ها آبی رنگ هستند.

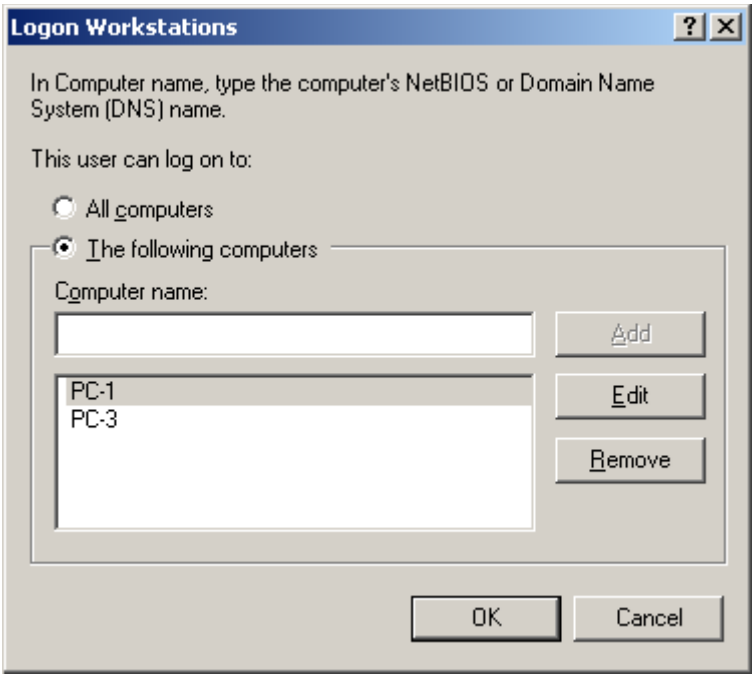


۲۲-۴-۴- Log On To

با انتخاب این گزینه می توانید برای کاربران محدودیتی ایجاد کنید که بر اساس این محدودیت، برخی کاربران فقط از طریق کامپیوتر هایی خاص بتوانند اقدام به Login کردن بکنند. بدین منظور در سربرگ Account روی دکمه Log On To کلیک کنید. در صفحه باز شده، مشخص است که کاربر از هر سیستمی می تواند Login کند.



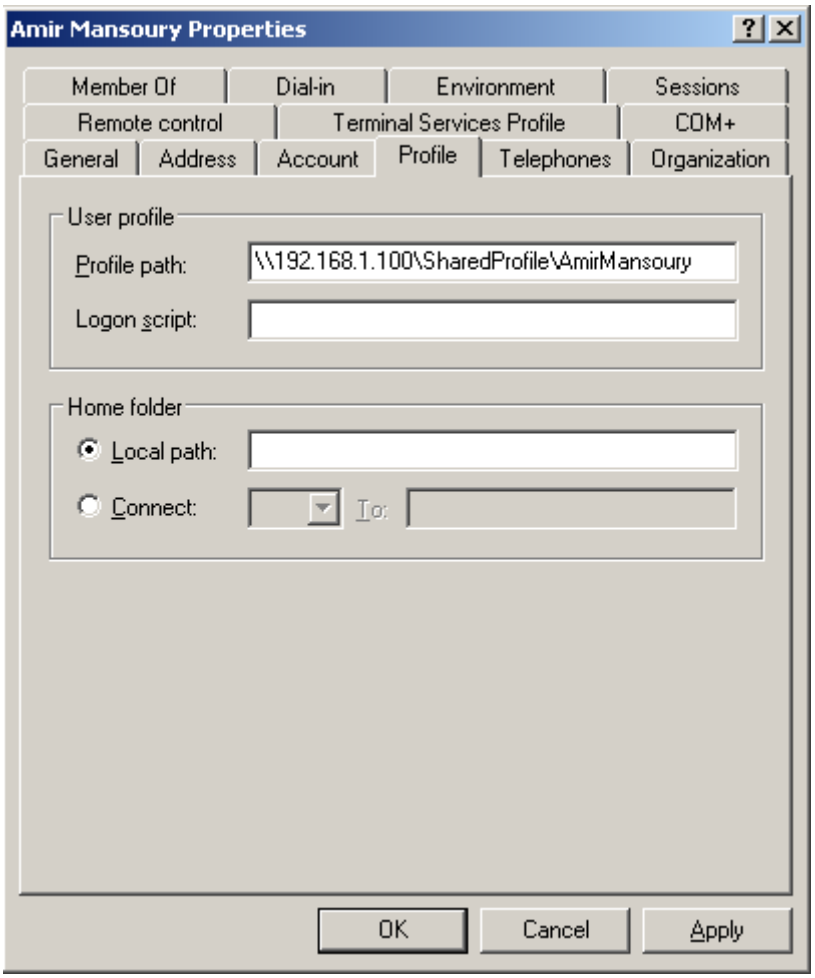
اما اگر خواستید که کاربر را محدود به سیستم هایی خاص کنید، ابتدا گزینه The following computers را فعال کرده و سپس **نام** کامپیوتر های مورد نظر (**Hostname**) را Add نمایید. مثلاً بر اساس شکل زیر، کاربر فقط می تواند از سیستم های PC-1 و PC-3 به سیستم Login کند.



Profile –۵–۴–۲۲

شما در این بخش این امکان را دارید که برای هر کاربر مشخص نمایید که فایل های شخصی و مرتبط با آن در جایی خاص قرار بگیرد و آن فرد از هر طریقی در هر کجا که به سیستم Login کند، بتواند به آنها دسترسی داشته باشد. مثلاً اگر فایلی Shortcut را روی صفحه دسکتاپ خود قرار داد یا چینش نوار استارت خود را تغییر داد، این تغییرات را از هر سیستمی که Login می کند، بتواند ببیند. بدین منظور ابتدا در کامپیوتر سرور، یک پوشه را Share کرده (توجه نمایید که کاربران این پوشه باید قابلیت Read و Write را داشته باشند. لذا در تنظیمات Permission این پوشه، به کاربر Every One، قابلیت Read و Write را بدهید.) و سپس در این پوشه، یک پوشه دیگر به نام کاربر قرار دهید. سپس در بخش Profile Path **آدرس پوشه Share شده در شبکه** را وارد نمایید. توجه: در اینجا نباید مسیر فیزیکی پوشه در سرور را وارد نمایید. بلکه باید مسیر پوشه Share شده که دیگر کاربران شبکه برای دسترسی به این پوشه، آن مسیر را وارد می کنند، وارد کنید. در این مثال، ما در مسیر D:\SharedProfile یک پوشه ساخته و آن را Share می کنیم. حال پوشه D:\SharedProfile\AmirMansoury را می

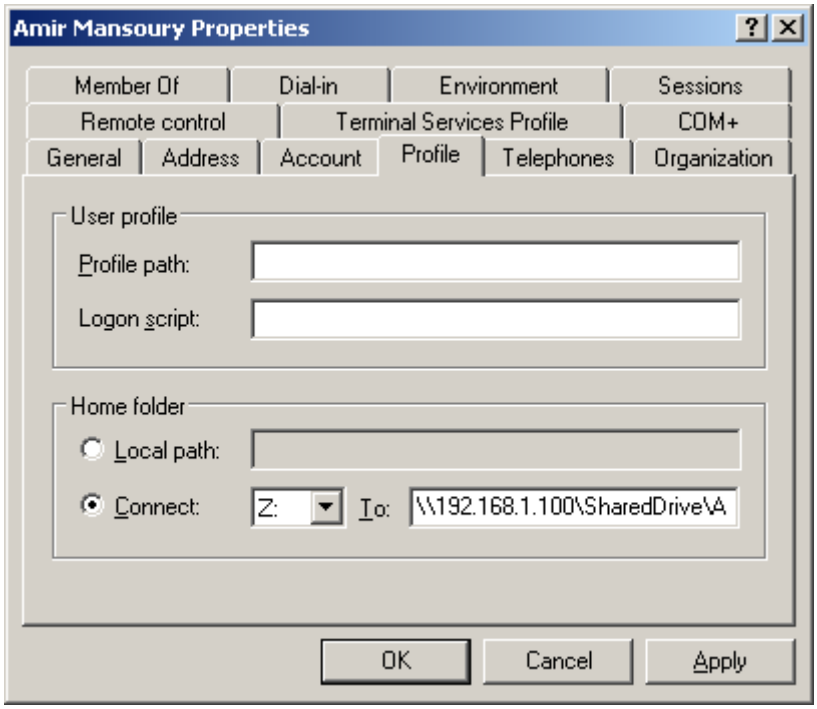
سازیم تا اطلاعات پروفایل کاربر در این پوشه قرار گیرد. حال بایستی مسیر پوشه Share شده در شبکه را وارد کنیم. با فرض اینکه آدرس IP سرور برابر ۱۹۲.۱۶۸.۱.۱۰۰ باشد، مسیر پوشه Share شده در شبکه برابر با \\192.168.1.100\SharedProfile\AmirMansoury خواهد بود.



۲۲-۴-۶- *Home Folder*

امکان دیگری که این سربرگ دارد این است: وقتی که کاربر به Domain وارد می شود، پشت هر سیستمی که باشد، درایو های دیسک سخت همان کامپیوتر را می بیند. به عنوان مثال اگر در درایو D:\ کامپیوتر PC-1 فایلی بسازد، سپس کاربر Logout کرده و اینبار با PC-3 وارد Domain شود، قادر به مشاهده فایل موجود در درایو D:\ نخواهد بود. ما در این بخش می خواهیم برای کاربر درایوی بسازیم که با هر سیستمی که Login کرد، بتواند این درایو را ببیند و اطلاعات آن در بین همه سیستم ها مشترک باشد. یعنی می خواهیم درایوی بسازیم که وابسته با کاربر باشد و نه وابسته به کامپیوتر.

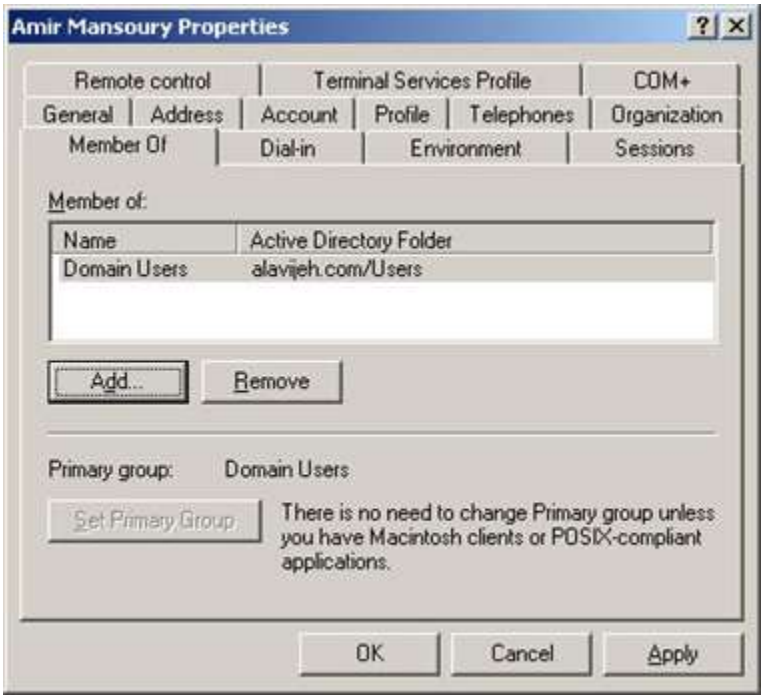
بدین منظور، مانند قسمت قبل، ابتدا در کامپیوتر سرور، یک پوشه را Share کرده (توجه نمایید که کاربران این پوشه باید قابلیت Read و Write را داشته باشند. لذا در تنظیمات Permission این پوشه، به کاربر Every One، قابلیت Read و Write را بدهید.) و سپس در این پوشه، یک پوشه دیگر به نام کاربر قرار دهید. سپس در بخش Connect، **آدرس پوشه Share شده در شبکه** را وارد نمایید. توجه: در اینجا نباید مسیر فیزیکی پوشه در سرور را وارد نمایید. بلکه باید مسیر پوشه Share شده که دیگر کاربران شبکه برای دسترسی به این پوشه، آن مسیر را وارد می کنند، وارد کنید. در این مثال، ما در مسیر D:\SharedDrive یک پوشه ساخته و آن را Share می کنیم. حال پوشه D:\SharedDrive\AmirMansoury را می سازیم تا اطلاعات پروفایل کاربر در این پوشه قرار گیرد. حال بایستی مسیر پوشه Share شده در شبکه را وارد کنیم. با فرض اینکه آدرس IP سرور برابر ۱۹۲.۱۶۸.۱.۱۰۰ باشد، مسیر پوشه Share شده در شبکه برابر با \\192.168.1.100\SharedDrive\AmirMansoury خواهد بود. همچنین در این قسمت باید مشخص نمایید که درایو ساخته شده، با چه حرفی نمایان شود. به صورت پیش فرض، این مقدار برابر Z:\ خواهد بود.



تنها نکته ای که باقی می ماند این است که با این کار، به صورت پیش فرض، کاربران هیچ گونه محدودیتی (از نظر میزان فضا) در استفاده از درایو خود ندارند و می توانند به حدی در آن اطلاعات بریزند تا درایو نگهدارنده این پوشه (در این مثال درایو D:\ موجود در سرور) پر شود. لذا بایستی کاربر را محدود کرد. بدین منظور بایستی از Disk Quota استفاده نمود. برای آشنایی با چگونگی این کار، به بخش Disk Quota در آخر همین فصل مراجعه نمایید.

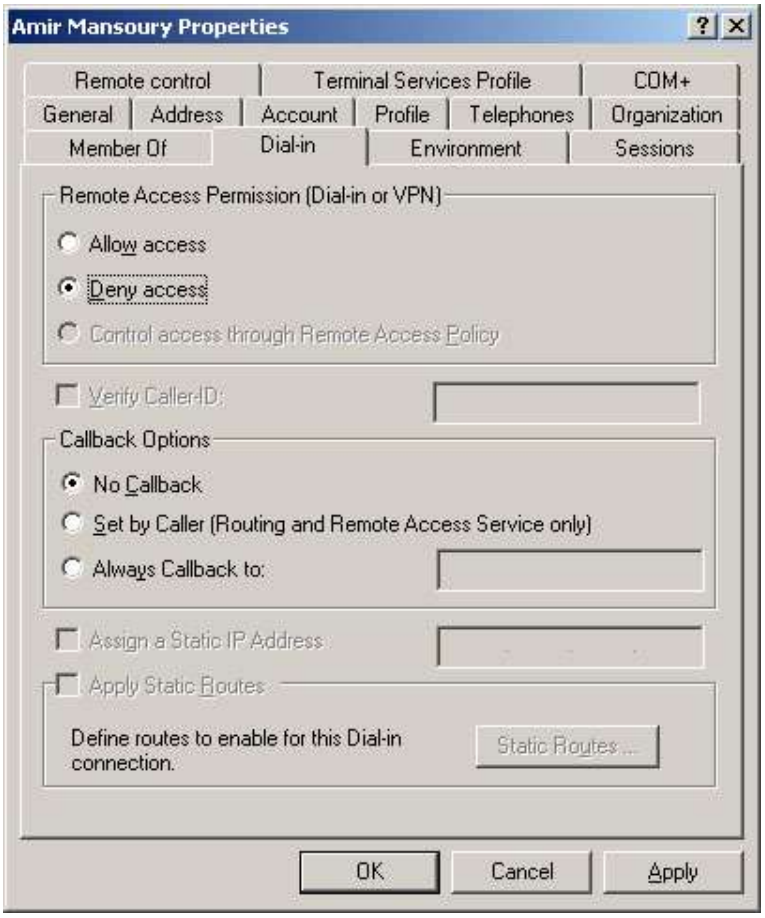
Member of – ۷-۴-۲۲

از طریق این سربرگ می توانید مشاهده کنید که کاربر عضو چه گروه هایی است. با کلیک روی دکمه Add، و سپس انتخاب یک گروه (گروه های) خاص، می توانید این کاربر را عضو این گروه (گروه ها) کنید. با کلیک روی دکمه Remove نیز کاربر از عضویت گروه خارج می شود.



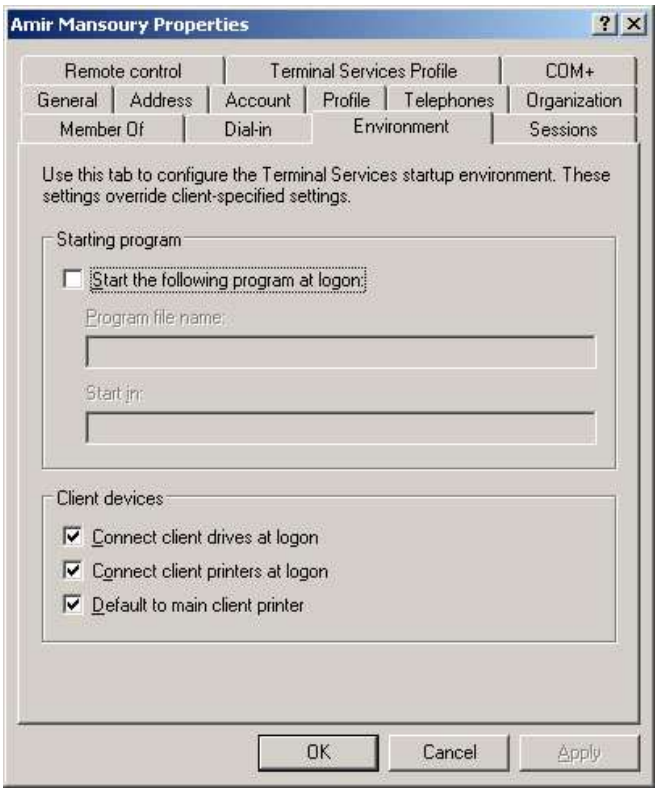
Dial-in – ۸-۴-۲۲

این بخش برای راه های اتصال به شبکه از راه های دیگر مثلاً به شیوه شماره گیری یا VPN میباشد. از طریق این قسمت می توانید تعیین کنید که آیا این کاربر قابلیت اتصال به شبکه از طریق شماره گیری یا VPN را دارد یا خیر؟ برای اطلاعات بیشتر به فصل VPN , Dialup مراجعه نمایید.



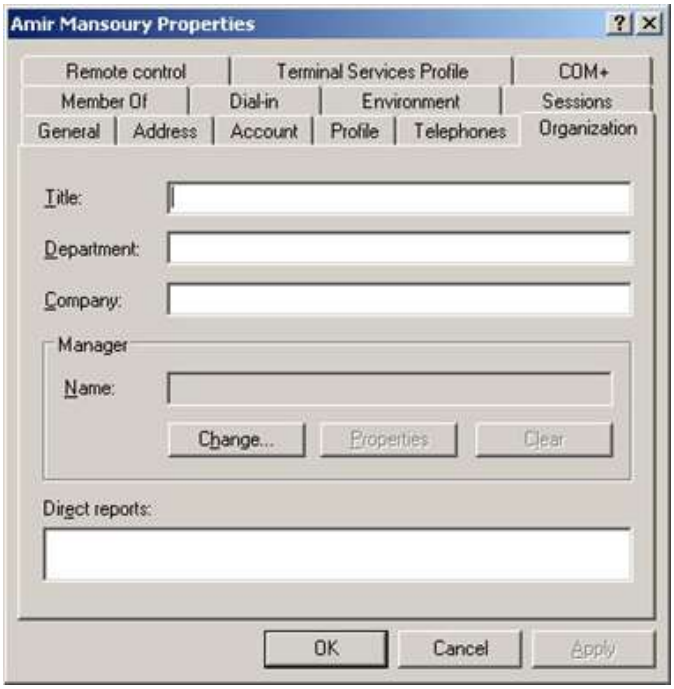
۲۲-۴-۹- *Environment*

در این بخش می توانید مشخص کنید که همزمان با Login کردن کاربر، چه برنامه ای برای آن کاربر شروع به اجرا شدن بکند. همچنین در Client Devices می توانید امکان استفاده از برخی تجهیزات سخت افزاری و استفاده از وسایل جانبی را به کاربر بدهید.



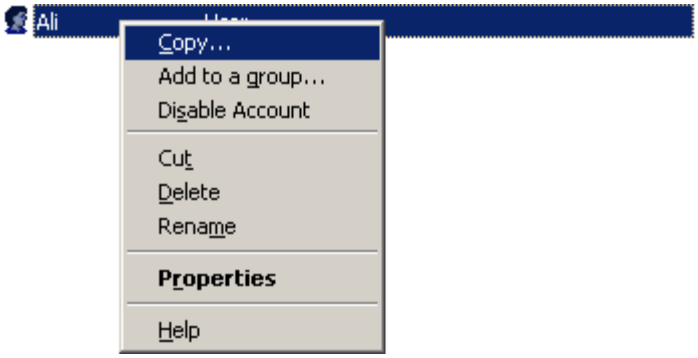
۲۲-۴-۱۰- Organization

در این بخش اطلاعات سازمانی کاربر وارد و مدیریت می شود (این اطلاعات سازمانی با بحث واحد سازمانی یا OU متفاوت است). از قبیل سِمت کاری، نام شرکت و همچنین واحد کاری که کاربر در آن مشغول به کار است.

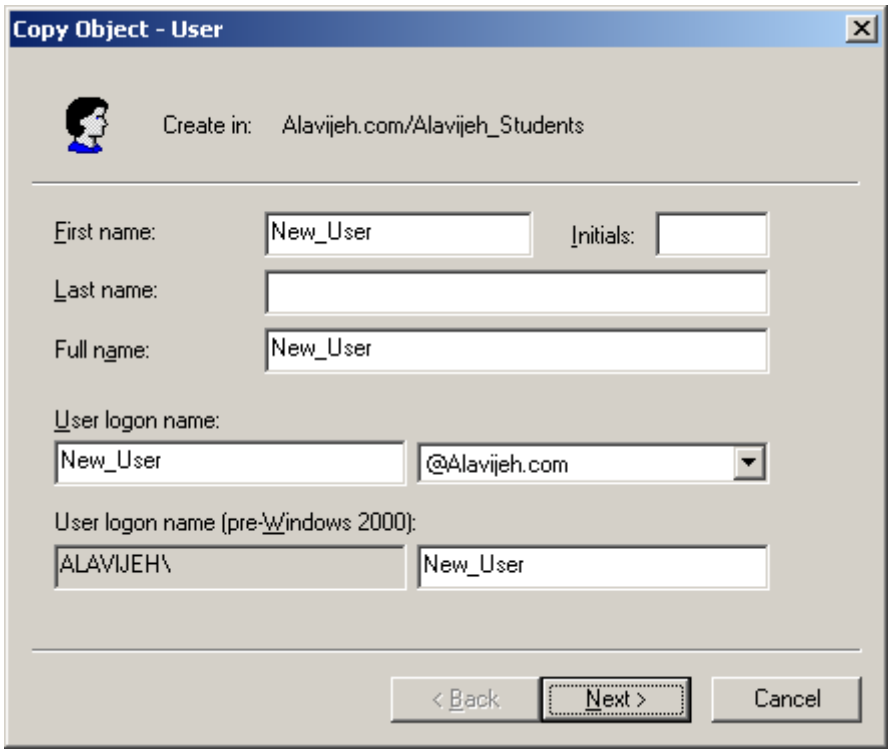


۲۲-۴-۱۱- تکثیر کاربران

فرض کنید نیاز داریم تعداد زیادی کاربر بسازیم که تمامی این کاربران ویژگی ها و سیاست ها و دسترسی های مشترک دارند. اینکه بخواهیم که کاربران را تک تک تعریف نموده و ویژگی های هر یک را نیز تک تک تعریف کنیم، کمی سخت و با ضریب اشتباه بالا می باشد. راه عاقلانه این می باشد که یک کاربر بسازیم (مثلاً به اسم User_Temp) و تنظیمات را روی آن اعمال کنیم. سپس کاربر مورد نظر را Disable می نماییم (به دلیل مسائل امنیتی حتما کاربر مذکور را غیر فعال نمایید). سپس هر گاه به کاربری نیاز داشتید که مشخصاتش معادل یا شبیه این کاربر باشد، می توانیم از این کاربر یک کپی بگیریم و کاربر جدید را فعال سازیم. بدین منظور روی نام کاربر مرجع راست کلیک نموده و گزینه Copy را انتخاب نمایید.



سپس صفحه ای باز می شود و مشخصات کاربر جدید را می خواهد. توجه داشته باشید که تمام اطلاعات کاربری کاربر قدیمی (مانند سطوح دسترسی، سیاست ها و ...) برای کاربر جدید نیز کپی می شود؛ و نیازی به تنظیم مجدد آن نمی باشد.



۵-۲۲- آشنایی با انواع گروه های Biult-in

گروه های Biult-in، گروه های هستند که بطور پیش فرض در زمان نصب Active Directory ایجاد می شوند؛ که بطور خلاصه برخی از آنها را معرفی می کنیم.

Builtin Global User

این نوع گروه ها در پوشه Users و در ابزار Active Directory Users and Computers قرار داشته و عبارتند از:

۱. **Domain Users**: این گروه شامل تمامی کاربران Domain است. هر کاربری که در Domain ایجاد می شود، به صورت خودکار به عضویت این گروه در آمده و می تواند از هر کامپیوتری به Domain وارد شود. اگر می خواهید که کاربری از راه دور نتواند به Domain وارد شوند و برای وارد شدن به Domain از خود کامپیوتر DC استفاده کند، وی را از عضویت این گروه خارج کنید.

۲. **Domain Administrators**: اعضای این گروه می توانند Domain را مدیریت کنند. این افراد به عنوان مدیر Domain شناخته می شوند. فقط Administrator مربوط به همان Domain، به صورت پیش فرض عضو این گروه می باشد.

Built-in Domain Local

این گروه ها در پوشه Built-in در ابزار Active Directory Users and Computers قرار دارند که عبارتند از:

۱. **Administrators**: اعضای این گروه می توانند DC ها را مدیریت کنند. این اعضا تمامی مجوز ها بر روی این کامپیوتر ها را دارا می باشند.

۲. **Account Operators**: اعضای این گروه عملیات مدیریتی همچون ایجاد، حذف و... را روی Account ها انجام میدهند. بطور مثال می توانند یک گروه را ایجاد و کاربرانی را به عضویت آن گروه در بیاورند.

۳. **Print Operators**: اعضای این گروه می توانند چاپگر های Domain را مدیریت کنند.

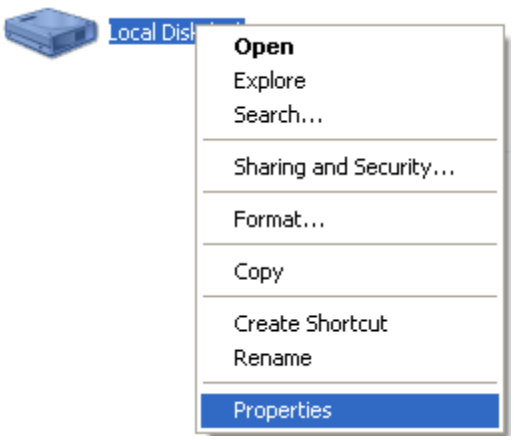
۴. **Backup Operators**: اعضای این گروه می توانند عملیات Backup گرفتن از اطلاعات و برگرداندن اطلاعات (Restore کردن) را انجام دهند.

۲۲-۶- آموزش کار با Disk Quota

Disk Quota امکانی است در ویندوز که به کمک آن می توان به تمام کاربران یک مجموعه یا به تعدادی از کاربران، یک مقدار خاص از فضای هارد دیسک اختصاص داد. در این صورت، آن ها قادر به استفاده بیشتر، از فضای تعیین شده نمی باشند.

توجه: این امکان فقط بر روی پارتیشن های که به فورمت NTFS هستند کار می کند.

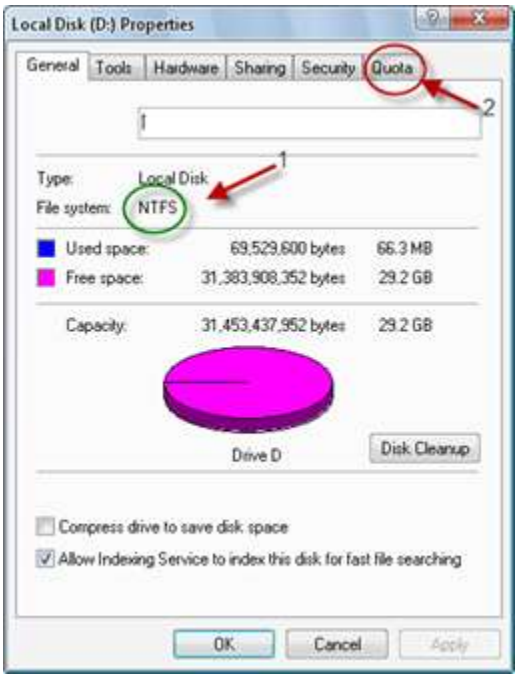
برای شروع کار، بر روی پارتیشنی که می خواهید این کار را انجام دهید کلیک راست کرده و گزینه Properties را انتخاب کنید.



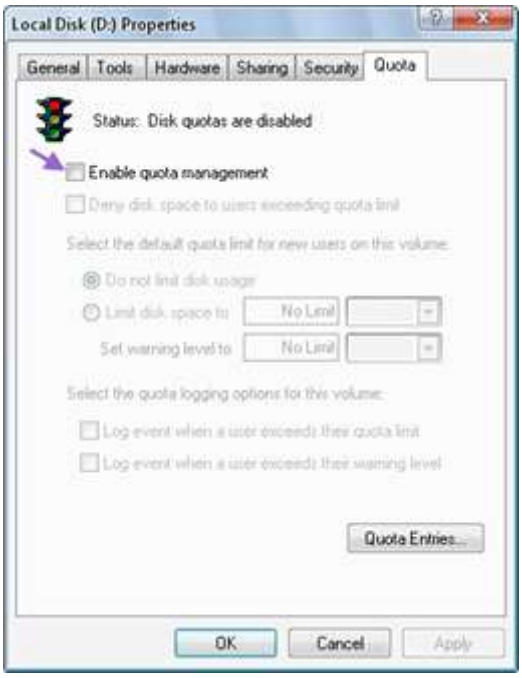
بعد از انتخاب این گزینه، شکل زیر باز می شود که شما باید کار های زیر را انجام دهید.

۱. باید توجه داشته باشید فرمت پارتیشن شما NTFS باشد.

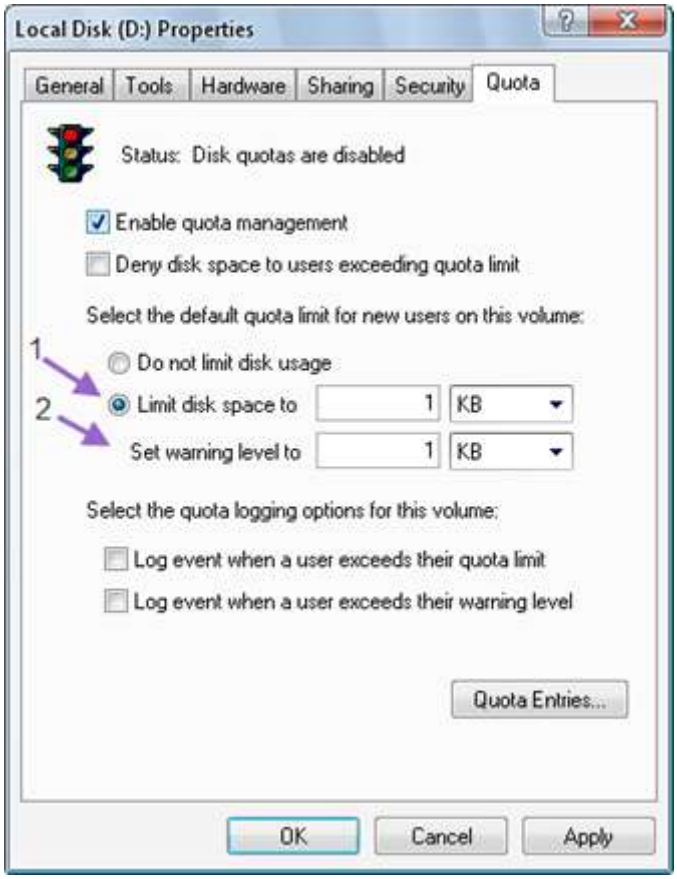
۲. سربرگ Quota را انتخاب کنید.



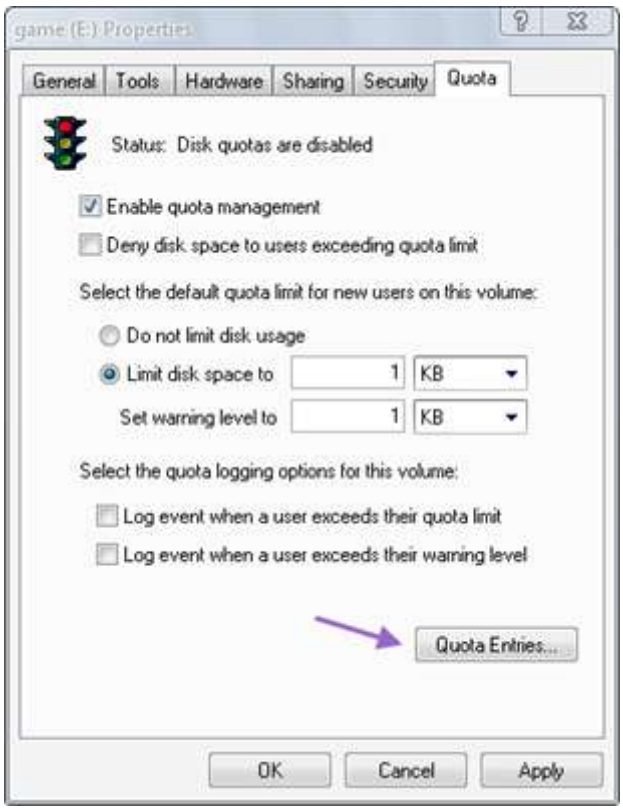
در این شکل، طبق فلش، گزینه Enable quota management را فعال کنید.



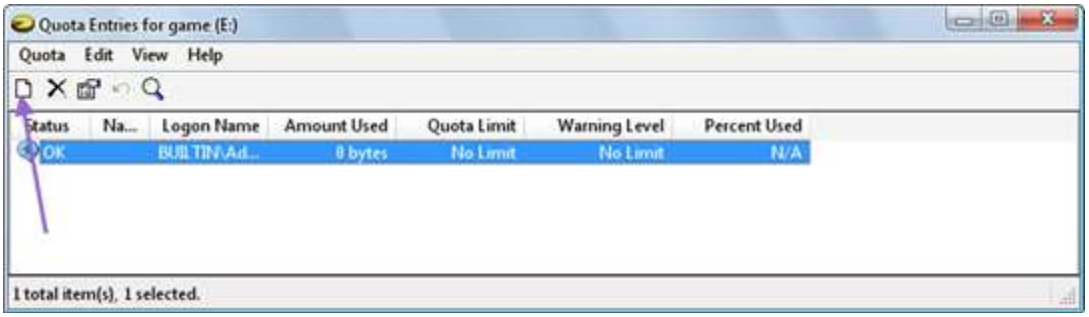
طبق شکل زیر، با انتخاب گزینه اول شما می توانید حداکثر فضایی که می خواهید به کاربران بدهید را وارد کنید و در گزینه دوم نیز می توانید عددی را وارد کنید که اگر فضای کاربر از آن عبور کرد، سیستم اخطار دهد.



مقدار فضایی که در شکل قبل تعیین، روی تمام کاربران اعمال می شود. اگر می خواهید به کاربری خاص، مقدار فضای دیگری را بدهید، در همین صفحه روی دکمه Quota Entries کلیک کنید.

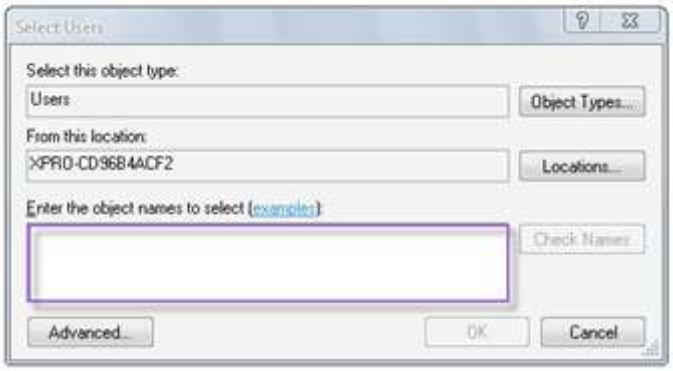


در صفحه باز شده، طبق شکل بر روی گزینه New کلیک کنید.

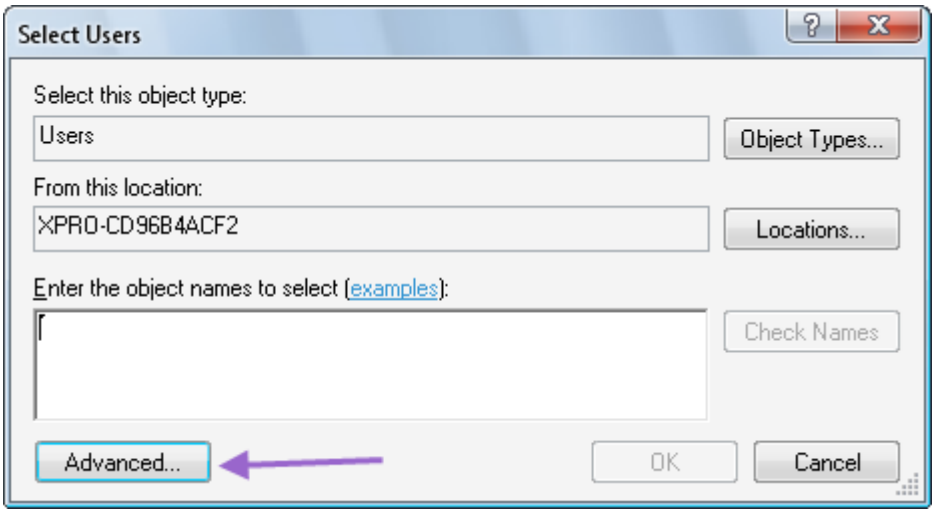


در صفحه باز شده، شما باید نام کاربر مورد نظر را وارد کرده و تایید کنید.

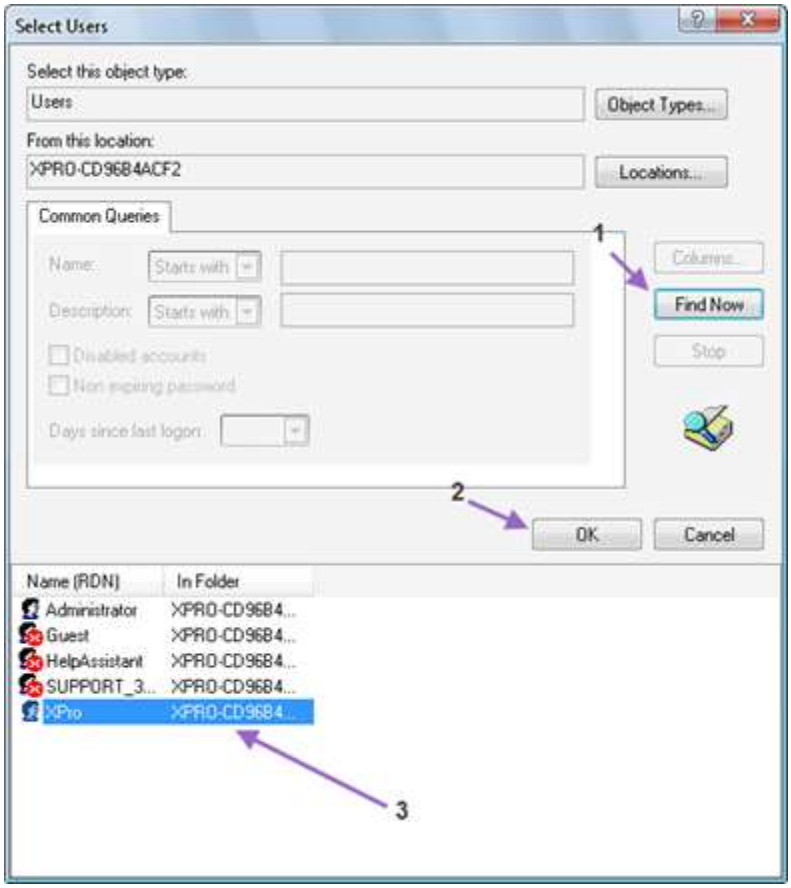
توجه: اگر شما مدیر ویندوز نباشید نمی توانید برای دیگر کاربران، فضا تعیین کنید.



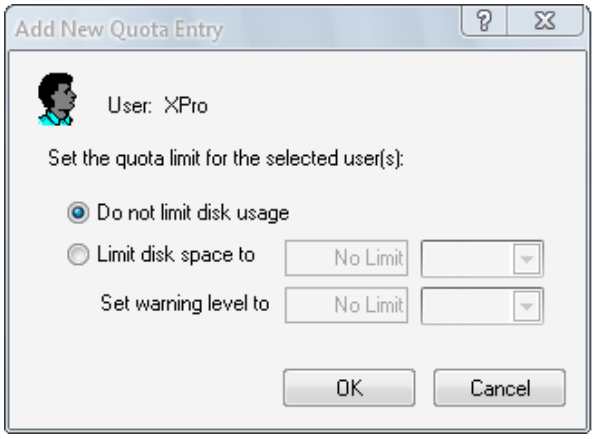
اگر نام کاربر را نمی دانید، طبق شکل ابتدا روی دکمه Advanced کلیک کنید.

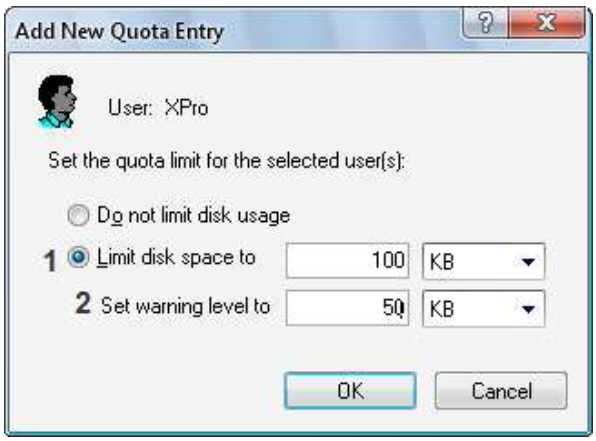


سپس روی دکمه Find کلیک کرده، کاربر(کاربران) مورد نظر را انتخاب کرده و در نهایت روی OK کلیک کنید.



حال اگر می خواهید کاربر(کاربران) انتخاب شده، محدودیتی در استفاده از فضای دیسک نداشته باشند، گزینه Do not limit disk usage، و اگر می خواهید محدودیتی روی فضای قابل استفاده آن ها ایجاد کنید، ابتدا گزینه Limit disk space to را فعال کرده و سپس مقادیر مورد نظر را وارد نمایید.





پس از تایید، کاربر جدید به لیست اضافه شده و شما می توانید آن را ببینید.

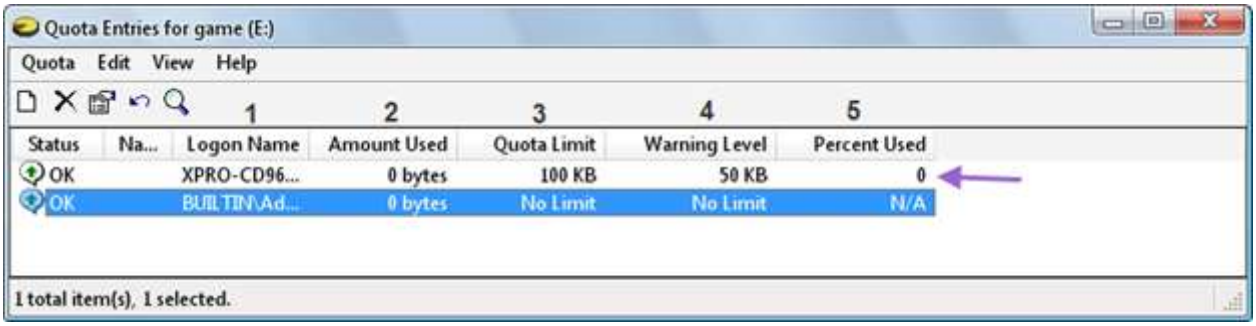
در شماره ۱ اسم کاربر نمایش داده می شود.

در شماره ۲ کل فضای استفاده شده نمایش داده می شود.

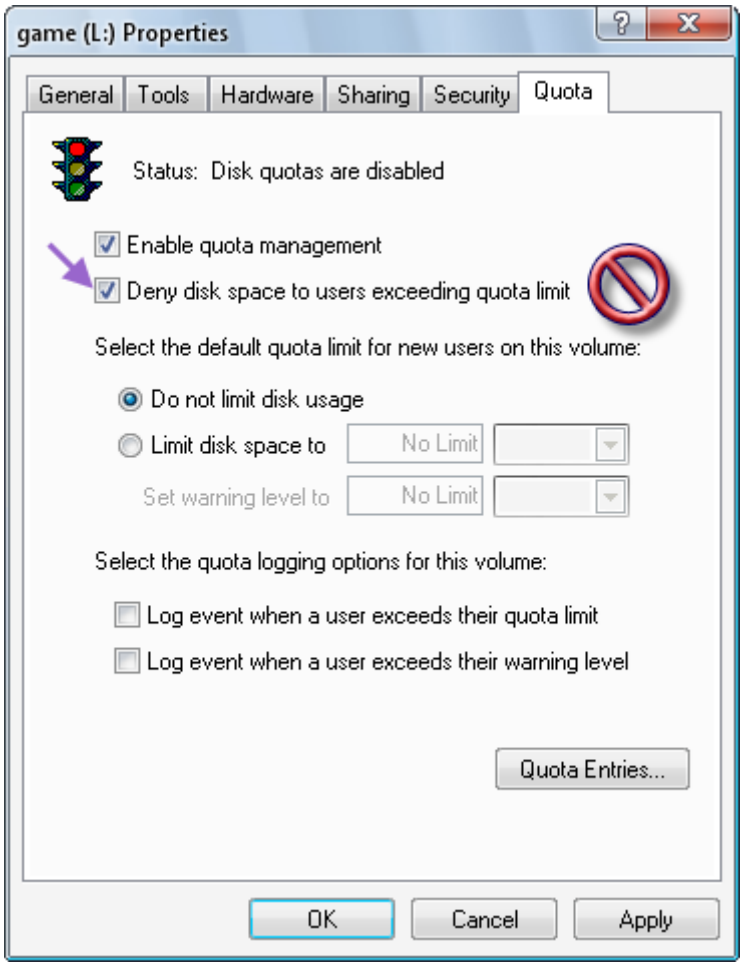
در شماره ۳ کل فضای اختصاص داده شده به کاربر نمایش داده می شود.

در شماره ۴ اگر کاربر از حد مجاز تعیین شده عبور کند، اخطار می دهد.

در شماره ۵ درصد استفاده شده از کل فضا را نشان می دهد.



این کار فقط در حد مانیتورینگ است. و برای عملی کردن این کار باید طبق شکل زیر عمل کرد.



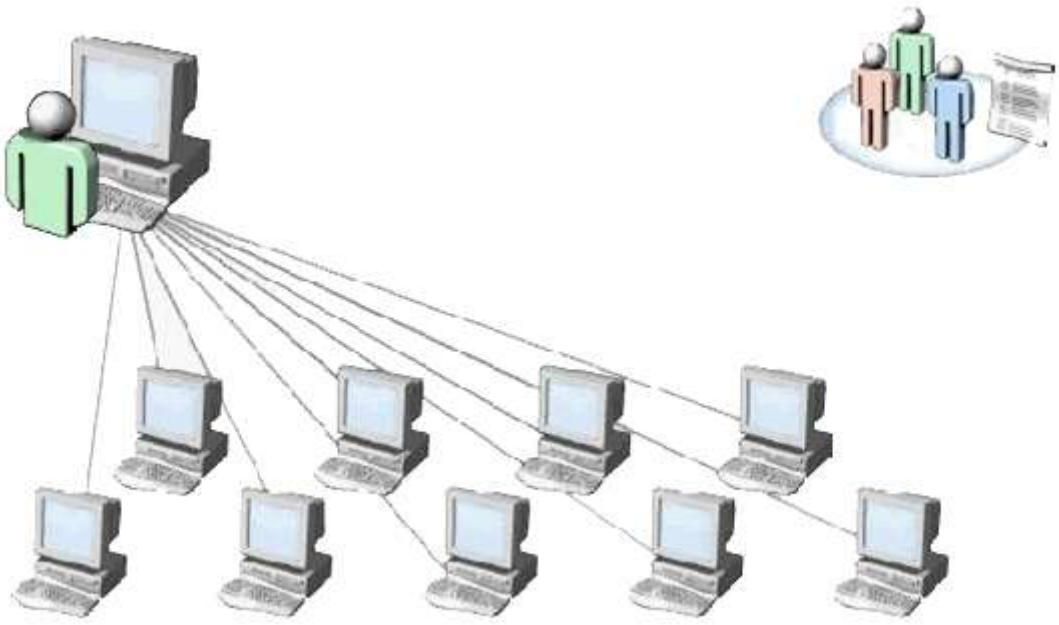
در این شکل با تیک زدن جای مشخص شده تمام کاربران انتخاب شده توسط شما به مقدار فضایی که دارند محدود می شوند.

فصل ۲۳

Group Policy

۲۳-۱- تعریف Group Policy

وقتی صحبت از قلب ویندوز به میان می آید، عموما تصویری از Registry در ذهن ایجاد می شود. Registry ابزار قدرتمندی است که قلب و هسته اصلی اعمال تغییرات در ویندوز است. اما در این بین Group Policy نیز ابزاری حیاتی و در عین حال ساده و User Friendly (کاربر پسند) است که میتواند تغییرات بسیار جامع و کاملی را شامل شود. در مقایسه با Registry می توان گفت که سادگی کار و وجود توضیحات کافی Group Policy را برتر از Registry جلوه می دهد.Group Policy در ویندوز سرور ۲۰۰۳، یک روش کارآمد و مفید به منظور مدیریت متمرکز و انجام تنظیمات بر روی Clientها می باشد. Group Policy به سرور ها و مدیران شبکه قدرت تنظیم و اعمال اجباری سیاست های خود بر روی کاربران و کامپیوتر هایی که به عنوان Client در شبکه قرار دارند را می دهد.



برخی از سیاست ها که توسط Group Policy بر روی کامپیوتر، کاربر یا گروهی خاص و بدون دخالت کاربر و از روی سرور انجام می شود عبارتند از:

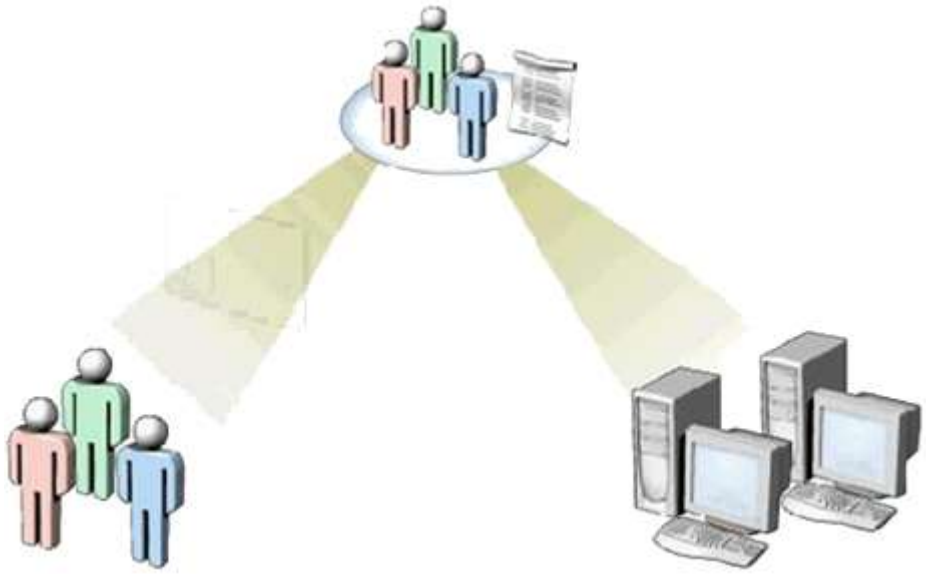
۱. نصب برنامه های کاربردی روی سیستم
۲. تنظیم اجباری رجیستری به تفکیک کاربر یا به تفکیک کامپیوتر (منظور دستگاه Clientی که به شبکه Login می کند)
۳. تنظیمات موارد امنیتی (Security Setting)

۴. اجرای اسکریپت هایی هنگام Log in یا Log off
۵. اجرای اسکریپت هایی هنگام بالا آمدن یا خاموش شدن سیستم
۶. حذف و اضافه نمودن گزینه ای Taskbar و Start Menu و کنترل پانل
۷. برخی تنظیمات برای سرویس هایی که از راه دور نصب می گردند.

به عبارت دیگر یک مدیر شبکه با این امکان به جای اینکه روی تک تک سیستم ها تنظیماتی را انجام دهد، می تواند از طریق سرور و برای گروه های مختلف سیاست های گوناگون را تنظیم و اعمال نماید؛ به طوری کاربر هیچگونه دخالتی در این خصوص نداشته باشد.

نکته: دقت کنید که تنظیمات Group Policy تنها بر روی سیستم عامل های Windows XP Professional، Windows 2000 و Windows Server 2003 اعمال می شوند و بر روی ویندوز های قدیمی نظیر خانواده 9X و یا Millennium پیاده سازی نخواهند شد.

برخی از تنظیمات Group Policy مخصوص کاربر و برخی دیگر از تنظیمات مخصوص کامپیوتر است. یعنی اگر تنظیمات روی کاربر اعمال گردد، آن کاربر از هر کامپیوتری که وارد شبکه گردد، آن سیاست ها و تنظیمات روی وی اعمال می شود و به کامپیوتر بستگی ندارد و برخی از سیاست ها Policy) ها(که روی کامپیوتر اعمال می شود به کاربر بستگی ندارد.



یک کامپیوتر با ویندوز سرور، به صورت پیش فرض، یک Local Group Policy دارد و می تواند تعدادی NonLocal Group Policy نیز داشته باشد.

– **Local Group Policy:** حتما با معنای واژه Local آشنایی دارید؛ یک Local Group Policy یعنی Group Policy هر کامپیوتر در خودش ذخیره شود و در واقع زمانی چنین روشی اتخاذ می شود که در محیط Active Directory Domain نیستیم. یک Local Group Policy فقط روی همان کامپیوتری که در آن قرار دارد اعمال می شود و nonLocal Group Policy ها ارجحیت بیشتری نسبت به Local Group Policy ها دارند. حال اگر در محیط دامنه Active Directory باشیم، سیاست های nonLocal ارجحیت بیشتری بر سیاست های Local دارند. پس اهمیت Local Group Policy زمانی است که کامپیوتر در یک شبکه بدون Active Directory حضور دارد. محل ذخیره سازی این تنظیمات ٪Systemroot%\System32\GroupPolicy است.

– **Non-Local Group Policy:** این سیاست ها باید در Active Directory ساخته شوند و به یک Site، Domain، OU مرتبط شوند. به صورت پیش فرض، با نصب Active Directory، دو Group Policy ساخته می شوند که عبارتند از:

۱. **Default Domain Policy**: این سیاست روی تمام دامنه (Domain) شامل کامپیوتر ها، Userها و Domain Controllerها اعمال می شود.

۲. **Default Domain Controllers Policy**: این سیاست روی تمام OU Domain Controller اعمال می شود. یادآوری می کنم که حساب Domain Controllerها روی یک OU جدا به نام Domain Controller نگه داری می شود. در صورتی که جای پوشه sysvol مقدار پیش فرض باشد، این سیاست ها در %Systemroot%\Sysvol\Domain Name\Policies\GPO GUID\Adm% ذخیره می شوند که که در این آدرس GUID یک ID یکتا است.

نکته مهم: یک GPO که برای یک سایت تعریف شده باشد، روی تمام کامپیوتر های آن سایت اعمال می شود. بنابراین، بدون توجه به دامنه ای که آن کامپیوتر در آن عضو است، می توان یک Group Policy اعمال کرد. (بدیهی است در یک جنگل باید باشند)

۲۳-۲- نحوه فعال شدن Group Policy

ابزار متداول ویرایش Group Policy، نرم افزار Group Policy Object Editor است. آنکه چگونه این ابزار را باز کنید، به این بستگی دارد که این سیاست ها به کجا قرار است اعمال شود و نوع Group Policy چیست.

۱. LGPO - Local Group Policy Objects:

- در RUN وارد کنید MMC و از منوی file گزینه Add/Remove Snap-In را انتخاب کنید.
- در زبانه Standalone Tab در صفحه Add/Remove Snap-In دکمه Add را بزنید.
- Group Policy Object Editor را Add کنید و دقت کنید که Local Computer انتخاب شده است.
- Finish را بزنید و سپس با زدن OK صفحه را ببندید.

نکته: با استفاده از GPedit.msc می توانید وارد LGPO شوید. از این رو، گاهی در لغت GPedit را به جای GPOE به کار می برند که منظور همان GPOE است.

۲. LGPO روی کامپیوتر دیگر:

- مراحل ۱ را انجام دهید با این تفاوت که با جای Local Computer، کامپیوتر دلخواه را انتخاب کنید.

۳. GPO روی یک سایت:

- به Administrative Tools بروید و کنسول Active Directory Site & Services را باز کنید.
- در درخت کنسول (نوار سمت چپ کنسول) روی سایتی که می خواهید Group Policy اعمال کنید، کلیک راست کنید و Properties را بزنید.
- به زبانه (Tab) مربوط به Group Policy بروید و برای اضافه کردن یک GPO گزینه Add را بزنید. می توانید برای ویرایش موارد موجود Edit را بزنید و ...

۴. GPO روی یک OU یا دامنه:

- به Administrative Tools بروید و کنسول Active Directory Users & Computers را باز کنید.
- در درخت کنسول (نوار سمت چپ کنسول) روی دامنه یا OU که می خواهید Group Policy اعمال کنید، کلیک راست کنید و Properties را بزنید.
- به زبانه (Tab) مربوط به Group Policy بروید و برای اضافه کردن یک GPO گزینه Add را بزنید. می توانید برای ویرایش موارد موجود Edit را بزنید.

تنظیماتی که شما در Group Policy انجام می دهید درون Group Policy Object یا به اختصار (GPO) ذخیره می شود. با هم نگاهی کوتاه به تنظیمات درون GPO می اندازیم.

Administrative Templates:

محل انجام تنظیمات Windows Components، Desktop، Start Menu and Taskbar، Control Panel، Shared Panel و Network System می باشد.

برای مثال در این قسمت می توان از تنظیماتی همچون نحوه اجرای Welcome Screen، تنظیمات مربوط به درایور ها، Interface مربوط به کاربران و تنظیمات مربوط به Editing Registry می باشد.

Security:

قوانینی است که می توانیم بر روی یک کامپیوتر و یا چندین کامپیوتر اعمال کنیم و از منابع موجود بر روی شبکه محافظت کنیم. Security Setting می تواند اعمالی همچون نحوه شناسایی کاربران در شبکه و یا نوع منابعی که کاربران اجازه ی استفاده از آن ها را دارند، نوع اطلاعاتی که باید درون Event Viewer ذخیره گردد و هم چنین عضویت در گروه های مختلف را کنترل نماید.

Software Installation:

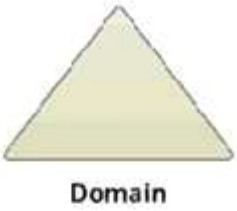
با استفاده از این گزینه می توانیم برنامه های مورد نظر را Install, Uninstall و یا پشتیبانی نماییم. با استفاده از Scripts، می توانید Scriptهایی را اختصاص دهید که به طور اتوماتیک در زمان خاموش و روشن شدن دستگاه و یا زمانی خاص اجرا شود. می توانید Scriptهای خود را به زبان های برنامه نویسی مختلفی که درون ویندوز پشتیبانی می شود مانند VB script یا Java script بنویسید.

Remote Installation Service:

این امکان را به شما می دهد که تنظیمات مربوط به نصب سیستم عامل را برای کاربران انجام دهید.

با استفاده از Internet Explorer Maintenance می توانید تنظیمات مربوط به نرم افزار IE و نحوه اجرای آن برای کاربران را مشخص نماید. از جمله این تنظیمات می توان از تنظیمات Proxy، اتصالات اینترنت و تنظیمات Security مربوط به Explorer را نام برد و در نهایت برای مدیریت اطلاعات مهم مانند محتویات Desktop وMy Document و سایر Folderهای مهم می توانید از گزینه ی Folder Redirection استفاده کرده و این Folderها را به یک محل خاص درون شبکه انتقال دهید و کاربران در تمامی حالات به آن دسترسی داشته باشند.

در ویندوز سرور، این امکان وجود دارد که Group Policy خود را به گروه هایی مهم همچون Site، Domain، Organizational Unit متصل و یا اصطلاحا لینک کنید. GPO (Group Policy Object) می تواند به بیش از یک قسمت لینک و یا اعمال شود. همچنین هر یک از این گروه ها می تواند به بیش از یک GPO متصل گردد. GPO بر اساس اولویتی که ماهیت ها و عناصر درون ساختار AD فعال می شوند، فعال می شود. به صورت پیش فرض GPO ابتدا بر روی Site، سپس Domain و در نهایت OU فعال میگردد. یعنی اگر روی OU سیاستی فعال کنید، سپس روی Domainی که OU عضو آن است، سیاستی متضاد با سیاست OU فعال کنید، **اولویت سیاست OU بیشتر بوده** و آن سیاست اعمال می شود، البته به شرطی که از سیاست اعمال شده Domain تجاوز نکند. مثلاً به Domain مقدار 1 GB فضا بدهیم، اما OU بخواهد از 2 GB فضا استفاده کند!



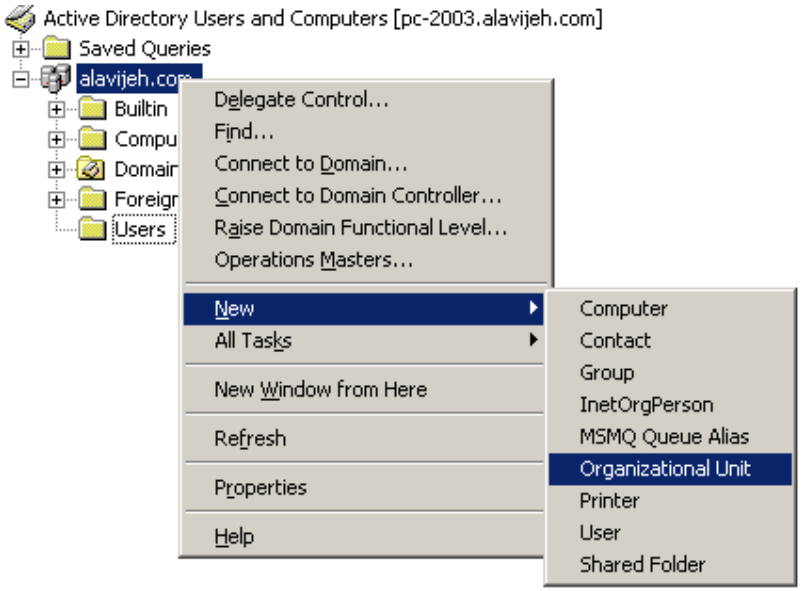
امروزه با توجه به گسترش و افزایش تعداد کاربران و کامپیوتر ها در شبکه، یک مدیر تنظیمات لازم را برای یک فرد یا یک کامپیوتر انجام نمی دهد، بلکه مدیر شبکه ابتدا گروه هایی ساخته و کاربرانی را عضو این گروه ها می کند و در این حالت می تواند سیاست ها و تنظیمات را رو ی این گروه ها اعمال کند. در این مقاله بر اساس امکانی که در ویندوز سرور ۲۰۰۳ وجود دارد، قصد داریم یک Organization Unit بسازیم (OU یا واحد سازمانی را مانند ظرفی در نظر بگیرید که هر چیزی می تواند در آن قرار گیرد، مانند کاربر، کامپیوتر، چاپگر و....) و تنظیمات را روی آن اعمال نماییم. پس ابتدا روش ساخت یک Organization Unit را شرح می دهیم.

۲۳-۳- ایجاد Organization Unit

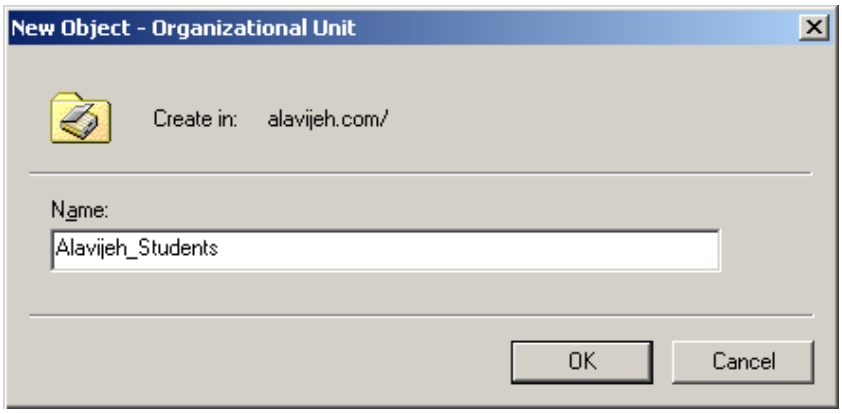
قبل از اینکه بخواهید Policy هایی را برای کاربران تعیین و اعمال نمایید و به منظور صرفه جویی در زمان یک Organization Unit ایجاد نمایید و کاربران مورد نظر را به عضویت آن در آورید تا نیاز نباشد برای هر کاربر جداگانه Group Policy تعریف و تنظیم شود. برای ساخت Organization Unit مراحل زیر را انجام دهید:

در قسمت Start بر روی Administrative Tools کلیک و سپس گزینه Active Directory Users and Computers را انتخاب نمائید.

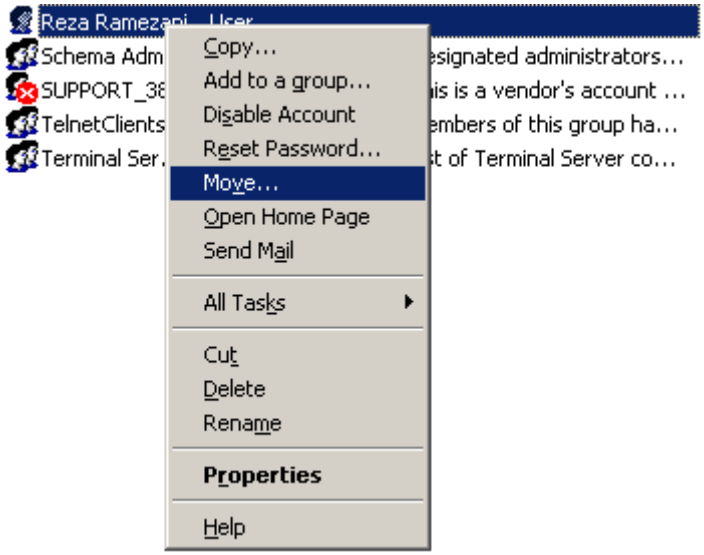
مطابق شکل زیر، روی نام سرور راست کلیک کرده و از منوی New گزینه Organization Unite را انتخاب نمایید.



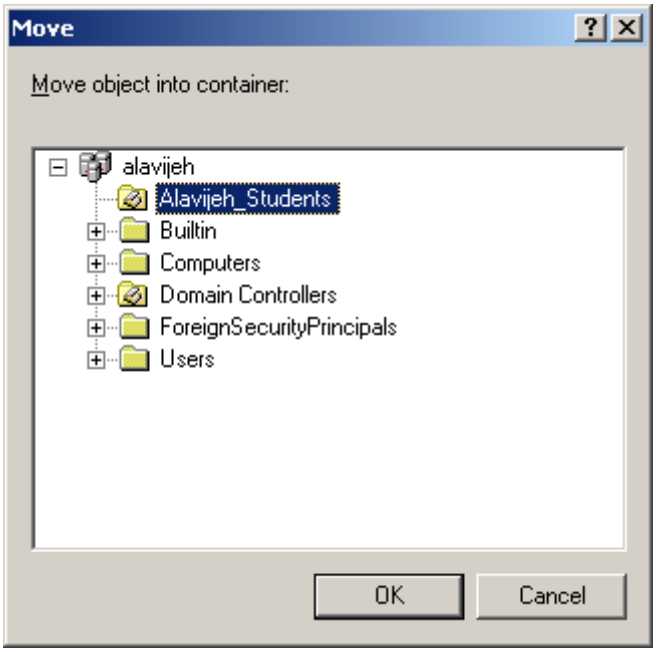
سپس یک نام برای واحد سازمانی خود (مثلاً Alavijeh_Students) وارد نمایید.



در ویندوز سرور ۲۰۰۳، هر کاربری که جدید ساخته شود به صورت پیش فرض در گروه Users قرار می گیرد پس برای اینکه بتوانید User یا Group ایجاد شده را عضو OU جدید کنید، آن را توسط موس داخل OU ساخته شده (در این مثال Alavijeh_Students) بیندازید. برای انتقال کاربر، روی آن راست کلیک کرده، گزینه Move را انتخاب کرده، مقصد را انتخاب نموده تا کاربر به آن انتقال یابد. در صورتیکه کاربری ایجاد نکرده اید بر روی Organization Unit ساخته شده راست کلیک کرده و از آنجا یک کاربر جدید بسازید تا از همان ابتدا عضو آن واحد سازمانی قرار گیرد.



انتخاب مقصد کاربر:



اکنون Organization Unit ساخته شده و اعضای آن نیز مشخص می باشند حال باید برای آنها Group Policy تعریف گـردد. برای درک مفهوم Group Policy و آشنایی عملی با آن، چند مثال را بطور عملی توضیح می دهیم.

۲۳-۴- مثال های عملی از Group Policy

در ادامه مثال هایی را در مورد چگونگی کار با Group Policy معرفی می نماییم.

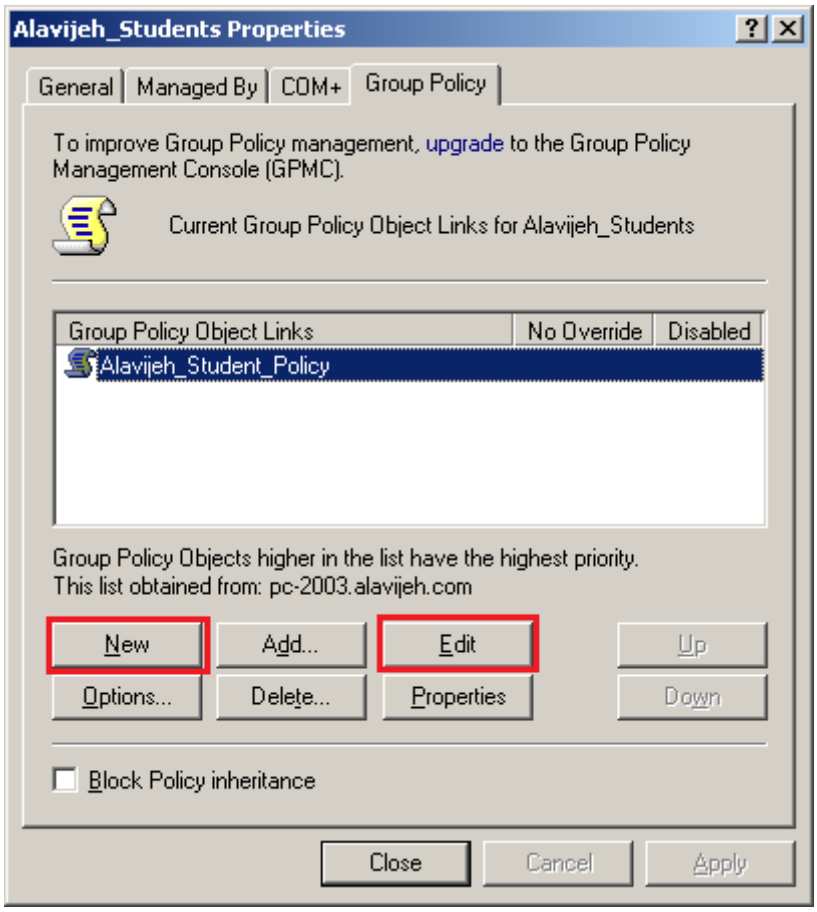
۲۳-۴-۱- تنظیم Proxy برای کاربران به صورت گروهی

فرض کنید در شبکه محلی (LAN) اداره یا سازمان متبوع خود، اینترنت راه اندازی کرده اید و می خواهید فقط برای گروهـی از کاربران و با استفاده از قابلیـت Group Policy پروکسـی (Proxy) تنظـیم نماییـد. اگـر شـبکه شـما دارای یـک Domain Controller (DC) باشد و همچنین Active Directory راه اندازی کرده اید، از این پس نیازی نیست برای تـک تـک کـاربران پروکسی تنظیم کنید. بلکه مراحل زیر را طی کنید:

روی Organization Unit ساخته شده راست کلیک و گزینه Properties را انتخاب نمایید

در صفحه ظاهر شده (در این مثال Alavijeh_Students Properties) به قسمت Group Policy بروید.

در این قسمت و مطابق شکل زیر دکمه New را بزنید و یک نام (مانند Alavijeh_Student_Policy) برای آن تعیین کنید.

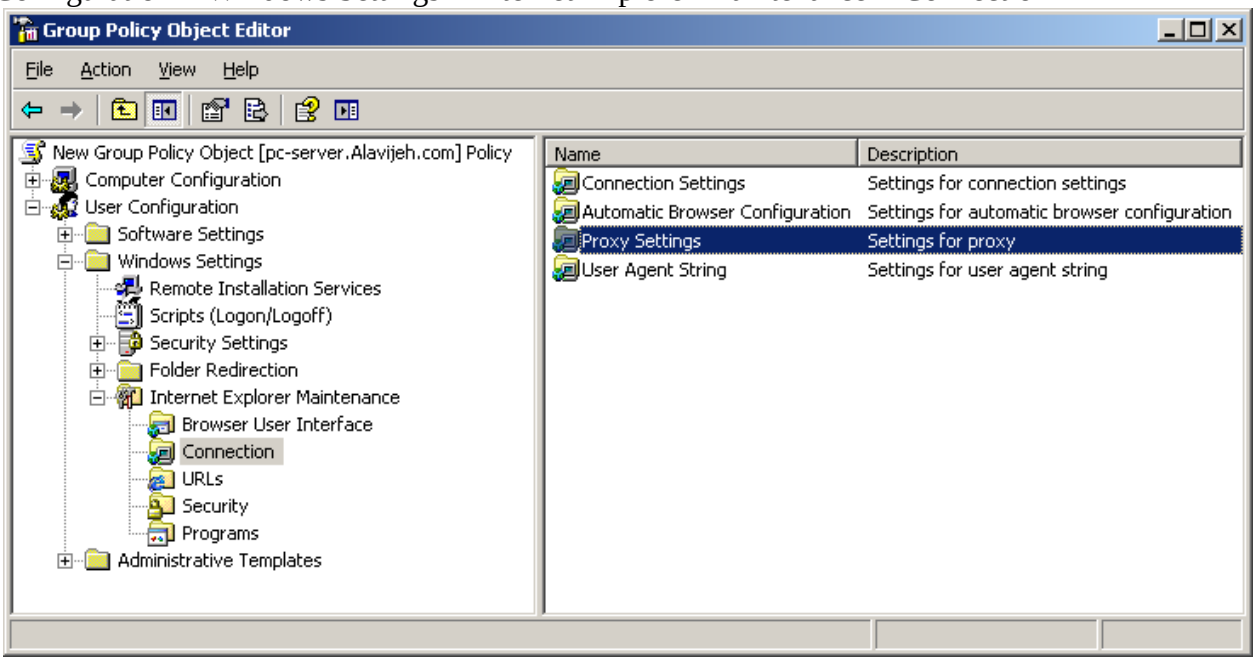


اکنون وقت تنظیم پروکسی می باشد. برای این منظور مراحل را به ترتیب زیر ادامه دهید:

در همان صفحه (مطابق شکل فوق)، Policy تعریف شده را انتخاب و گزینه Edit را بزنید

در صفحه Group Policy Object Editor به مسیر زیر بروید.

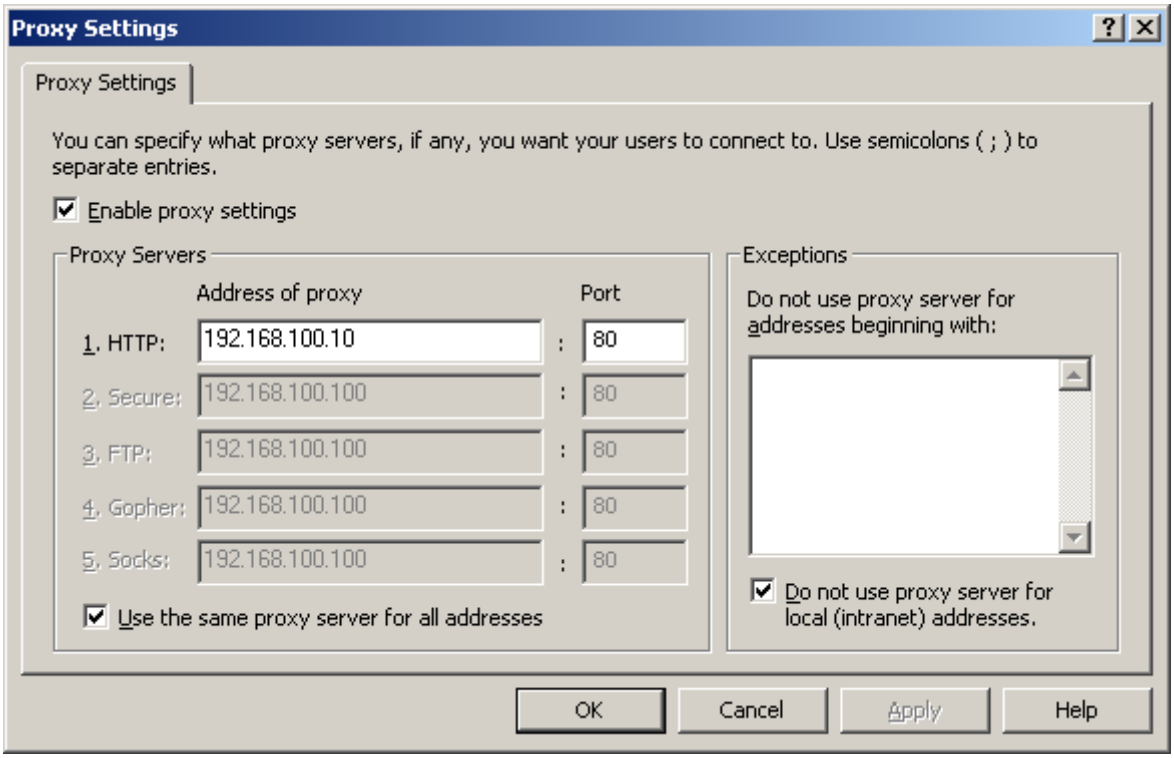
User Configuration➔Windows Settings➔Internet Explorer Maintenance➔Connection



در صفحه سمت راست گزینه Proxy Setting را انتخاب نمائید.

در صفحه Proxy Setting ابتدا تیک Enable Proxy Setting را بزنید (به شکل زیر توجه کنید)

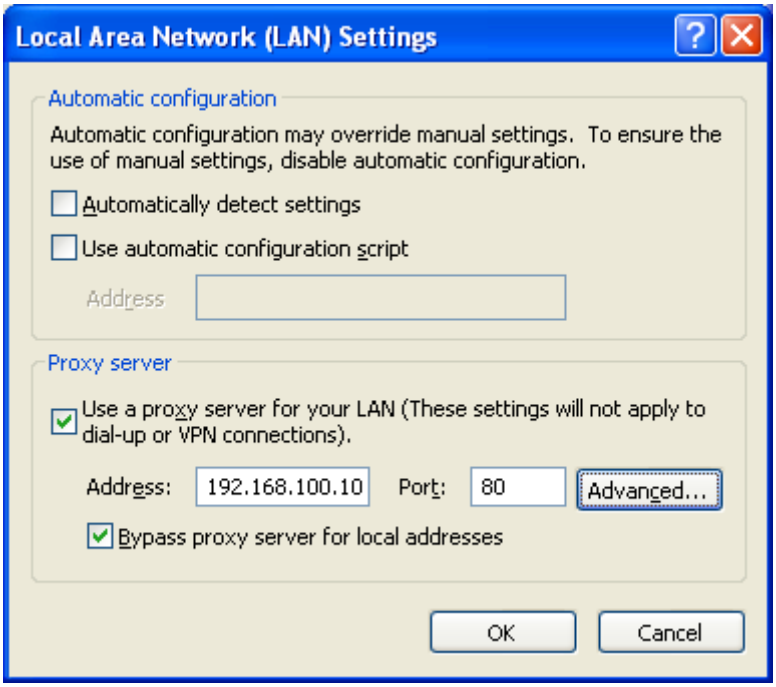
سپس مطابق شکل زیر، در قسمت HTTP آدرسی که قرار است کاربران به آن متصل شوند و اینترنت را از آنجا دریافت کنند را وارد کنید.



همانطور که در شکل زیر ملاحظه می کنید، از این پس، کاربرانی که با نام کاربری و رمز عبوری که در Domain موجود باشد به شبکه Login کنند و عضو Organization Unit ساخته شده توسط شما نیز باشند، به صورت اتوماتیک در Internet Explorer خود در قسمت Proxy Server آدرس ۱۹۲.۱۶۸.۱۰۰.۱۰ با پورت ۸۰ وارد شده است.

Tools➔Internet Options ➔ Connection ➔ LAN Setting ➔ Proxy Server

این همان آدرسی است که در قسمت قبل (به شکل فوق توجه کنید) تنظیم شده است.



۲۳-۴-۲- تغییر Title Bar اینترنت اکسپلورر

شاید بخواهید در صفحه Internet Explorer تمام کاربرانی که در شبکه محلی از اینترنت استفاده می کنند، نام سازمان یا اداره متبوع خود را در Title Bar بنویسید، به طوریکه هر کاربری که به شبکه با نام کاربری و رمز عبور معتبر در Domain وارد می شود و Internet Explorer را باز می کند نام سازمان را در بالای صفحه آن ببیند. برای تنظیم این مورد مراحل زیر را انجام دهید:

روی Organization Unit ساخته شده کلیک راست نمایید و گزینه Properties را بزنید.

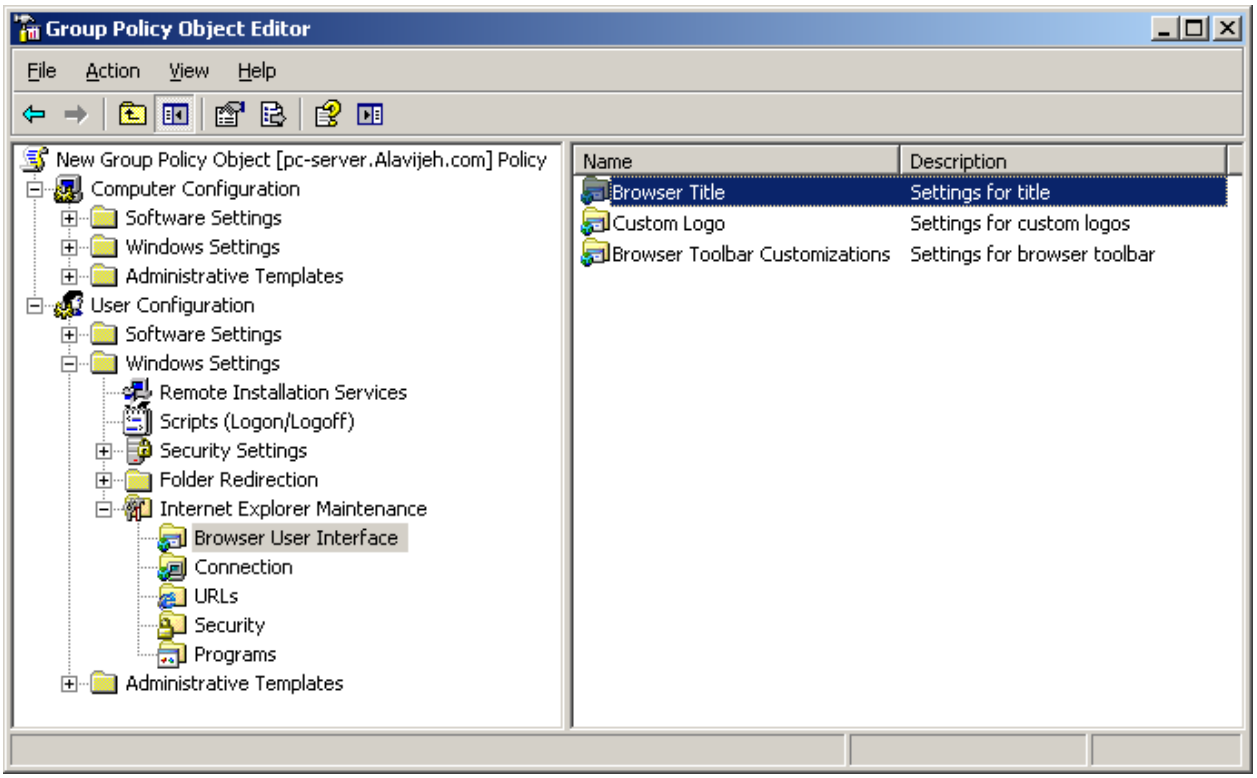
در صفحه ظاهر شده به قسمت Group Policy بروید.

Group Policy ای که در قسمت قبل ایجاد شد را انتخاب و مجدد دکمه Edit را بزنید.

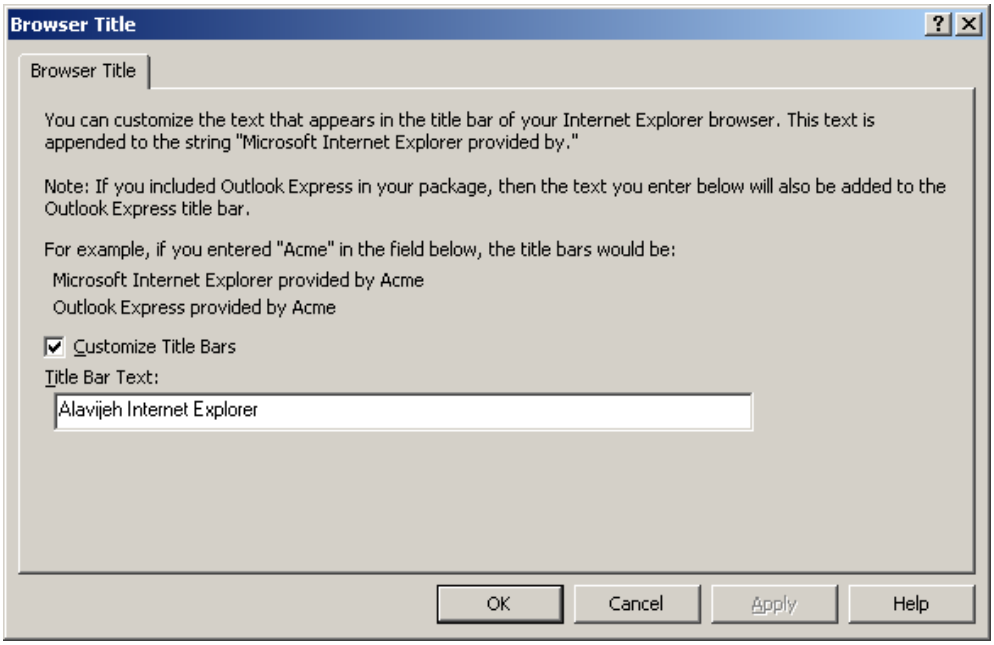
در صفحه Group Policy Object Editor به مسیر زیر بروید:

User Configuration➔Window Setting➔Internet Explorer Maintenance➔Brower User Interface

از صفحه سمت راست گزینه Browser Title را انتخاب کنید.



مطابق شکل زیر، ابتدا تیک مربوط به Customize Title Bars را زده و متن دلخواه خود را داخل Title Bar Text بنویسید.



برای دیدن نتیجه لازم است با Username و Password کاربری که عضو گروه ساخته شده است، به شبکه Login کنید تا نتیجه را مانند آنچه در شکل زیر آمده است، ملاحظه نمایید.

۲۳-۴-۳- تنظیمات نوار وظیفه و منوی شروع (Start Menu and Taskbar)

ویندوز کلیه تنظیمات مربوط به منوی شروع (Start Menu) و نوار وظیفه (Task bar) را در محل مشخصی از Group Policy قرار داده است که می توانید همه چیز در این دو مورد را در همان قسمت تنظیم نمایید.

به عنوان مثال شاید لازم باشد در شبکه محلی شما بنابر طراحی انجام شده، دکمه RUN روی منوی شروع کاربران نباشد یا نتوانند از شبکه خارج شوند، یعنی بخواهید به صورت مرکزی دکمه Log Off را از منوی شروع کلیه کاربران عضو یک گروه بردارید.

برای تنظیم کردن این موارد و براساس نیازتان مراحل زیر را انجام دهید:

روی Organization Unit ساخته شده راست کلیک کنید سپس دکمه Properties را بزنید

Group Policy ساخته شده را انتخاب و گزینه Edit را بزنید.

در صفحه Group Policy Object Editor به مسیر زیر بروید:

User Configuration➔Administrative Templates➔Start Menu Tools Bar

در پنجره ای که در سمت راست ظاهر می شود تنظیماتی مانند آنچه در زیر اشاره می شود را می توانید انجام دهید:

۱. حذف یا اضافه کردن دکمه RUN
۲. حذف یا اضافه کردن نام کاربری
۳. حذف یا اضافه کردن دکمه Log Off
۴. حذف یا اضافه کردن Shutdown و بسیاری تنظیمات دیگر.

در شکل زیر، نمونه های مختلف را مشاهده می نمایید:

Remove user's folders from the Start Menu	Not configured
Remove links and access to Windows Update	Not configured
Remove common program groups from Start Menu	Not configured
Remove My Documents icon from Start Menu	Not configured
Remove Documents menu from Start Menu	Not configured
Remove programs on Settings menu	Not configured
Remove Network Connections from Start Menu	Not configured
Remove Favorites menu from Start Menu	Not configured
Remove Search menu from Start Menu	Not configured
Remove Help menu from Start Menu	Not configured
Remove Run menu from Start Menu	Not configured
Remove My Pictures icon from Start Menu	Not configured
Remove My Music icon from Start Menu	Not configured
Remove My Network Places icon from Start Menu	Not configured
Add Logoff to the Start Menu	Not configured
Remove Logoff on the Start Menu	Not configured

Remove and prevent access to the Shut Down command	Not configured
Remove Drag-and-drop context menus on the Start Menu	Not configured
Prevent changes to Taskbar and Start Menu Settings	Not configured
Remove access to the context menus for the taskbar	Not configured
Do not keep history of recently opened documents	Not configured
Clear history of recently opened documents on exit	Not configured
Turn off personalized menus	Not configured
Turn off user tracking	Not configured
Add "Run in Separate Memory Space" check box to Run dialog box	Not configured
Do not use the search-based method when resolving shell shortcuts	Not configured
Do not use the tracking-based method when resolving shell short...	Not configured
Gray unavailable Windows Installer programs Start Menu shortcuts	Not configured
Prevent grouping of taskbar items	Not configured
Turn off notification area cleanup	Not configured
Lock the Taskbar	Not configured
Force classic Start Menu	Not configured

هر آیتمی در بخش Administrative Templates، سه حالت دارد:

۱. **Not Configured:** به معنای آنکه تغییر به Registry اعمال نشده است.
۲. **Enabled:** به معنای آنکه سیاست اثر گذار است و Registry تغییر یافته است.

۳. **Disabled:** به معنای آنکه تغییر یافته و سیاست اثرگذار نیست.

اما به عنوان مثال برای حذف دکمه RUN در همان پنجره روی گزینه Remove Run Menu From Start Menu دو بار کلیک کنید تا پنجره ای مطابق شکل زیر مشاهده شود.

در این پنجره اگر گزینه Enable را انتخاب کنید، دکمه Run برای کلیه کاربرانی که به شبکه وارد می شوند حذف می شود و یا برای اینکه دکمه Shut Down را از روی منوی شروع بر داریم، در همین قسمت گزینه Remove and Prevent Access to the Shutdown را فعال می کنیم.

۲۳-۴-۴- تنظیمات و حذف و اضافه گزینه های مربوط به Control Panel

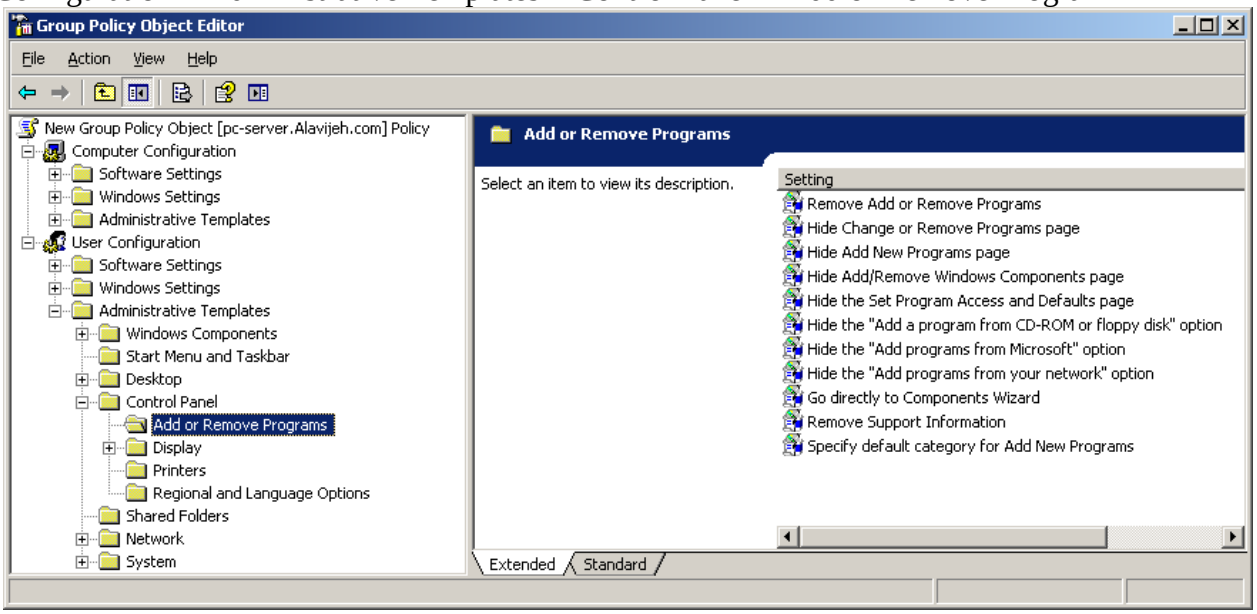
با توجه به تکرار مراحل قبلی که چندین بار به آن اشاره شد یعنی با Edit کردن Group Policy ساخته شده و در صفحه Group Policy Object Editor از طریق مسیر زیر می توان کلیه تنظیمات و محدودیت های مربوط به کنترل پانل را برای کاربران انجام داد.

User Configuration➔Administrative Templates➔Control Panel

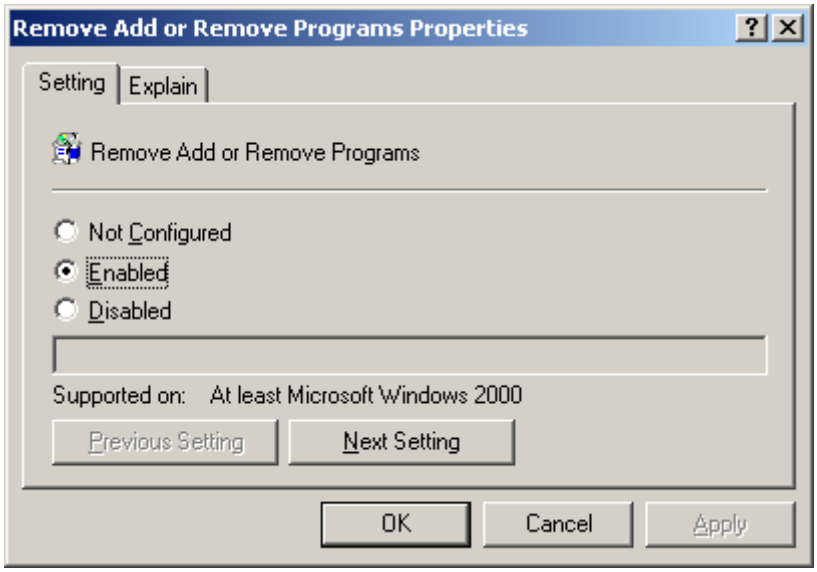
به عنوان مثال اگر بخواهید دکمه Add \ Remove Program از داخل کنترل پانل سیستم های موجود در شبکه حذف نمایید مراحل زیر را انجام دهید:

ابتدا به مسیر زیر بروید:

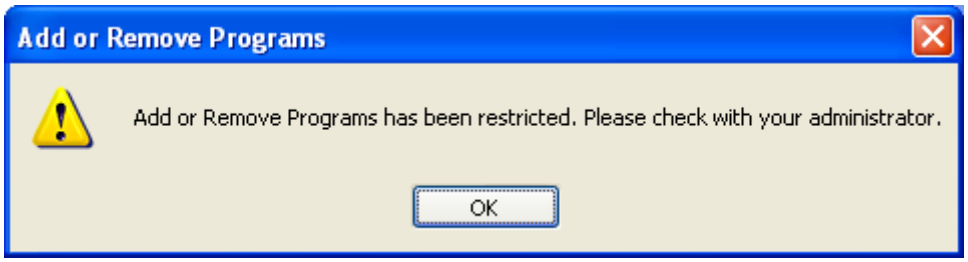
User Configuration➔Administrative Templates➔Control Panel➔Add or Remove Program



سپس از صفحه سمت راست، همانطور که در شکل زیر مشاهده می کنید، گزینه Remove Add or Remove Program را با دوبار کلیک انتخاب کنید و سپس در پنجره ای که باز می شود گزینه Enable را بزنید.



بعد از این تنظیم اگر کاربری که جزء گروه ایجاد شده (در این مثال Alavijeh_Students) باشد وارد Control Panel سیستم خود شود، با توجه Policy که در این مثال تعریف شده نمی تواند گزینه Add or Remove Program را اجرا نماید و در صورت اجرای آن، با پیغامی که در شکل زیر مشاهده می کنید مواجه می گردد.



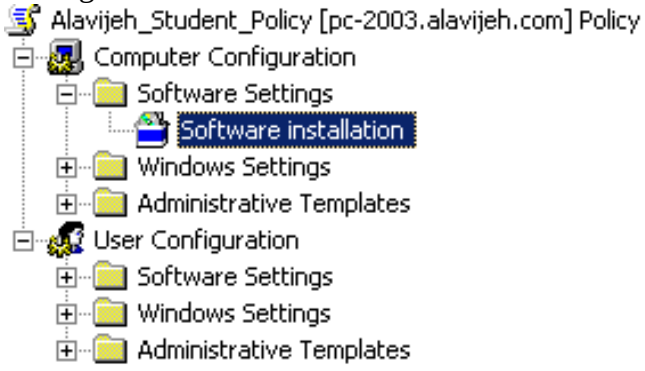
۲۳-۴-۵- نصب برنامه های کاربردی

می خواهیم برنامه ای را تعیین کنیم که تمامی کاربران بتوانند در شبکه نصب کنند. معمولاً آنچه که می خواهیم روی کامپیوتر های کلاینت نصب کنیم سه دسته می شوند:

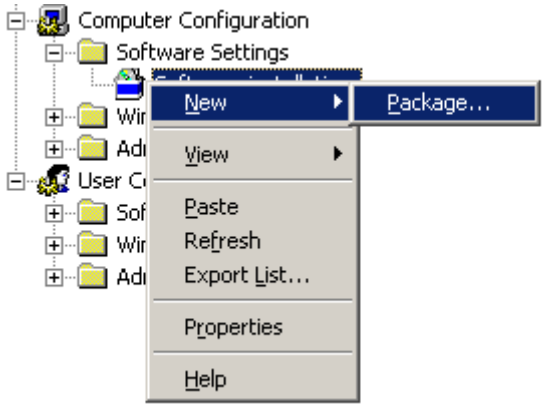
۱. فایل های MSU که مربوط به روز رسانی های ویندوز می باشند. آن ها را با WSUS منتشر می کنیم و در اینجا بررسی نمی شوند.
۲. فایل های MSI که با کمترین زحمتی قابل نصب روی تمام کلاینت های مورد نظر هستند و در اینجا روی این فایل ها تمرکز می کنیم.
۳. فایل های غیر از MSI مانند EXE که می خواهیم روی تمام کلاینت های مورد نظر نصب شوند و قدری کار بیشتر نیاز است.

بدین منظور مجددا مانند قبل وارد صفحه Edit ➔ Group Policy واحد سازمانی یا Domain ساخته شده شوید. سپس وارد مسیر زیر شوید:

User | Computer ➔ Software Settings ➔ Software Installation



سپس روی Software installation راست کلیک کرده و از قسمت New گزینه Package را انتخاب نمایید.

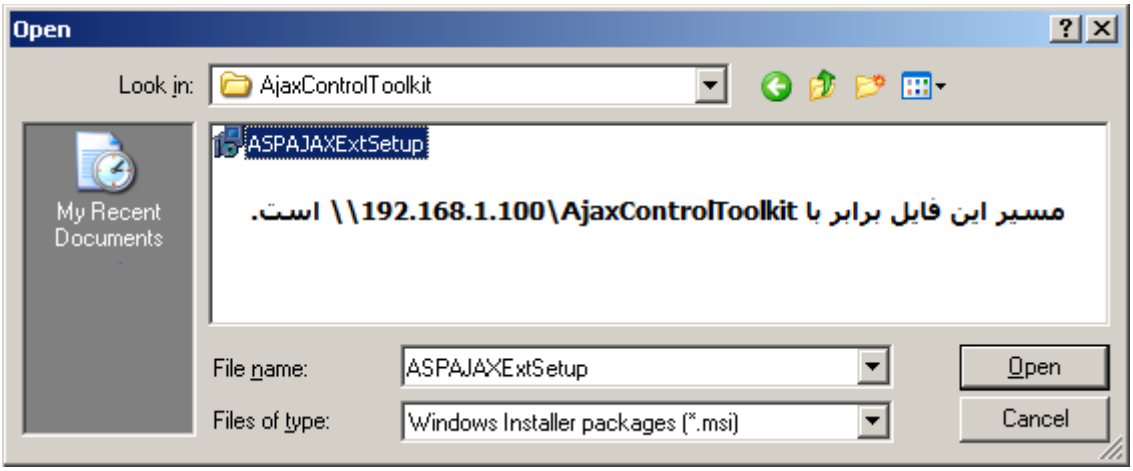


بر حسب آنکه نوع فایل MSI است یا نه، در اینجا باید مراحل مختلفی را انجام دهیم. اگر MSI باشد، فایل را انتخاب می کنیم و مراحل ساخت Package را ادامه می دهیم. اما اگر نوع فایل ZAP باشد، باید ابتدا یک ZAP فایل بسازیم که در ادامه توضیح می دهیم.

مهم: در هنگام انتخاب مسیر فایل Installation و ZAP فایل، **فراموش نکنید و تاکید می کنم فراموش نکنید** که مسیر فایل را در شبکه وارد کنید. مثلاً از طریق My Network Places مسیر را وارد کنید یا مثلاً :

\\Server1\office\word.msi

بنابراین بدیهی است که باید فایل ها Share باشند. البته اگر فراموش کنید، ویندوز با پیام هشداری به شما یادآوری می کند.



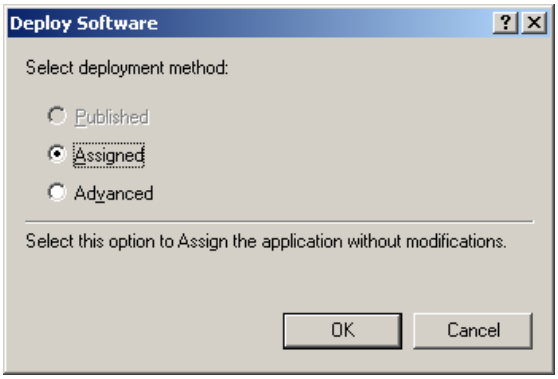
پس از ساخت Package سه گزینه در دسترس داریم:

- **Published** : اگر یک Package به صورت Published تنظیم شود، اولین باری که کاربر Login کند Add/Remove Program برای او نمایش داده خواهد شد و کاربر **می تواند انتخاب کند که برنامه نصب شود یا خیر.**
- **Assigned** : اگر یک Package به صورت Assigned به کاربری تنظیم شود، اولین باری که کاربر Login کند برنامه نصب می شود و پیش از اولین بار اجرا، نهایی می شود. اگر یک Package به صورت Assigned به کامپیوتری تنظیم شود، اولین باری که ویندوز Start می شود، Package نصب می شود و پیش از اولین اجرا نهایی می شود. برای تمام کاربران آن کامپیوتر نرم افزار قابل دسترسی خواهد بود.
- بدیهی است از آنجا که کامپیوتر ها نمی توانند تصمیم بگیرند که آیا یک Package نصب شود یا خیر، گزینه Published برای کامپیوتر ها غیر فعال است.
- فایل های ZAP فقط می توانند برای کاربران یعنی در قسمت User Configuration تنظیم شوند. چرا که فایل های ZAP از برنامه نصب کننده اختصاصی خود استفاده می کنند و نمی توانند از Elevated Privileges استفاده کنند.

بنابراین در هنگام نصب اگر Administrative Permission نیاز باشد، تنها کاربرانی که دارای این مجوز هستند می توانند این فایل را نصب کنند . بنابراین باید Published شوند تا کاربری مراحل نصب را انجام دهد.

- **Advanced:** تنظیمات اضافی را در اختیار قرار می دهد. بسیاری از نکات از جمله Advanced را فعلا صرف نظر می کنیم.

توجه : به نسخه های ۳۲ بیتی و ۶۴ بیتی توجه کنید.



(در این مثال، ما Package را روی Computer نصب کردیم، لذا گزینه Published غیر فعال است.)

ساختن یک ZAP فایل: Zap فایل، یک فایل متنی است و بنابر این می تواند به راحتی با Notepad و یا هر ویرایشگر متن دیگری نوشته شود. در اینجا یک مثال برای ساخت Zap فایل ارائه می دهیم.

مثال: به آسانی کد زیر را در NotePad نوشته و تغییرات لازم را انجام دهید و سپس آن را با پسوند Zap ذخیره کنید. در این مثال Excel 2007 را نصب می کنیم. دقت کنید که فایل را با پسوند Zap.txt به اشتباه ذخیره نکنید.

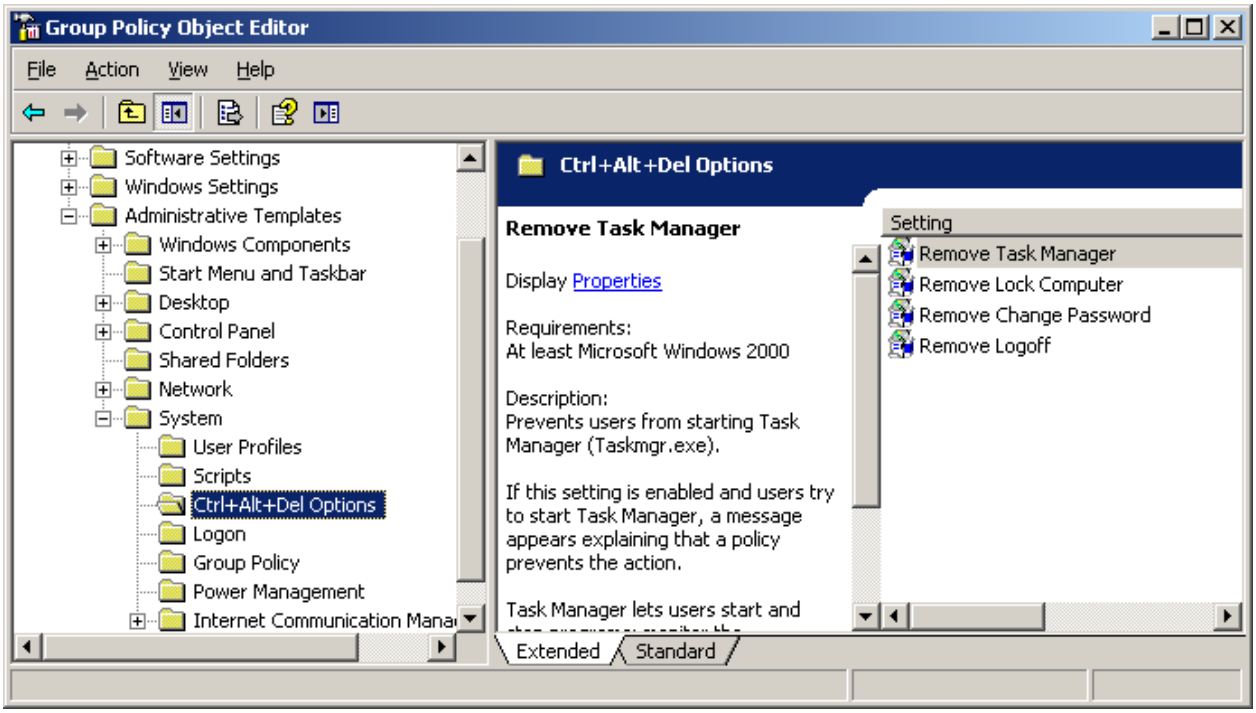
```
[Application]
FriendlyName = "Microsoft Excel 2007"
SetupCommand="\\server5\share\Excel 2007\setup.exe"
```

۲۳-۴-۶- غیر فعال نمودن Ctrl + Alt + Delete

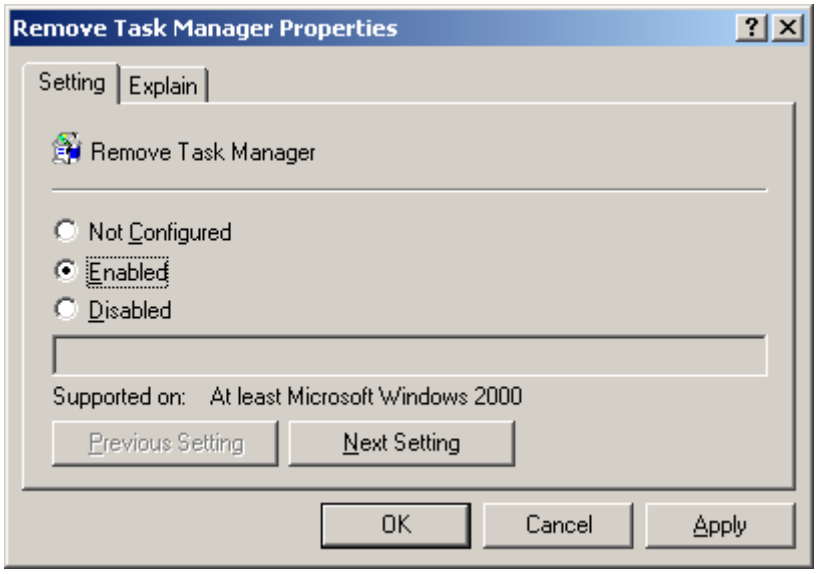
در بسیاری از موارد، نیاز داریم که امکان Ctrl + Alt + Delete را از کاربر بگیریم. بدین منظور ابتدا وارد Group Policy Object Editor شده و سپس به مسیر زیر بروید:

User Configuration ➔ Administrative Templates ➔ System ➔ Ctrl + Alt + Delete Options

سپس از صفحه سمت راست، گزینه Remove Task Manager را انتخاب کنید.



سپس در صفحه باز شده، گزینه Enabled را انتخاب نموده و سپس OK کنید.



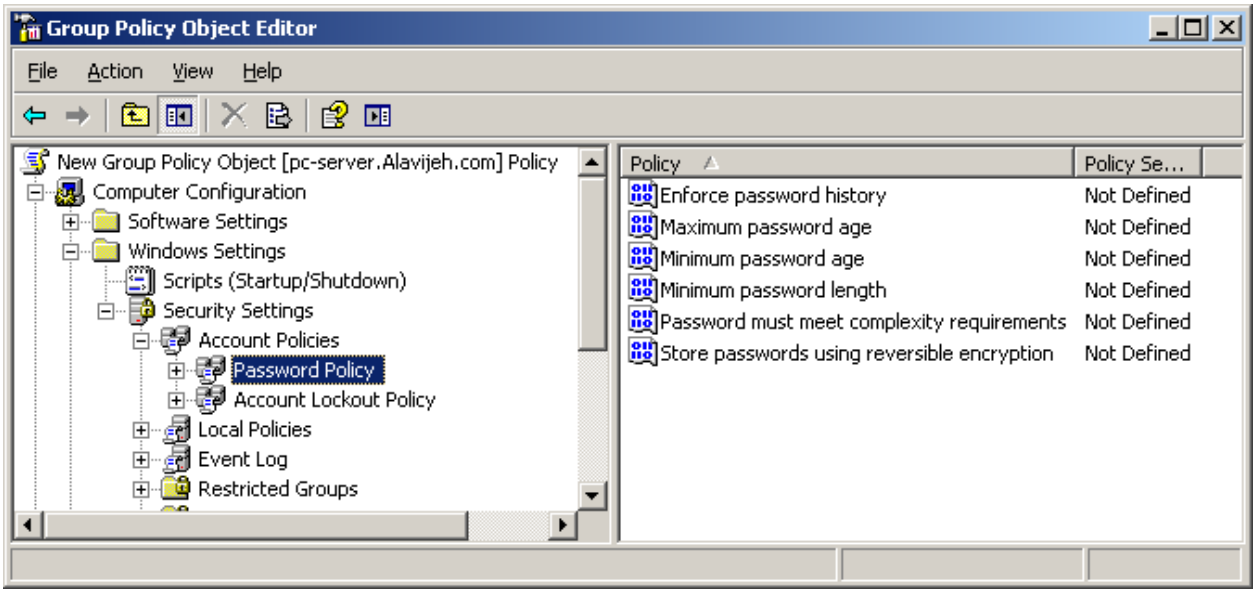
بدین ترتیب کاربرانی که این سیاست روی آن ها اعمال می شود، هنگام فشردن کلیدهای Ctrl + Alt + Delete قسمت Task Manager آن ها غیر فعال خواهد بود.

۲۳-۴-۷- امنیت رمز عبور کاربران

به عنوان آخرین مبحث آموزشی Group Policy، به بحث سیستم های امنیتی رمز عبور در Group Policy می پردازیم. بدین منظور ابتدا وارد Group Policy Object Editor شده و سپس به مسیر زیر بروید:

Computer Configuration➔Windows Settings➔Account Policies➔Password Policy

در سمت راست صفحه، تعدادی از سیاست ها را مشاهده می کنید که در ادامه به توضیح آن خواهیم پرداخت:

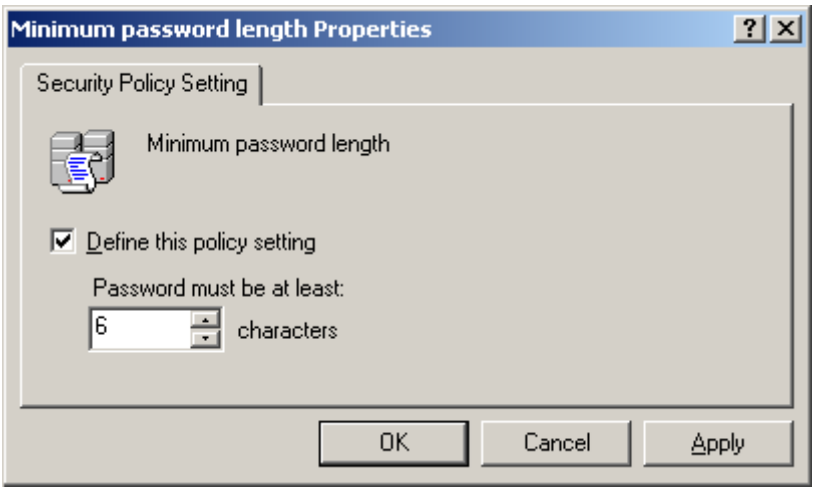


– **Enforce Password History**: توسط این قسمت می توان به سیستم گفت که رمز های عبور کاربر را (حتی رمز های قبلی کاربر که اکنون تغییر یافته است) همیشه نگهداری کند، حال هنگام تغییر رمز عبور کاربر، سیستم به وی اجازه نمی دهد که از n رمز عبور قبلی خود استفاده کند. در مثال زیر ما تعیین کرده ایم که کاربر نتواند رمزی مانند ۳ رمز قبلی خود وارد کند.

– **Maximum Password Age**: در این قسمت حداکثر طول عمر یک رمز عبور تعیین می شود و بعد از آن، رمز عبور Expire شده و کاربر بایستی رمز عبور خود را تغییر دهد. به طور پیش فرض این مقدار برابر با ۴۲ است. در اینجا ما مقدار را برابر ۳۰ در نظر گرفته ایم.

– **Minimum Password Age**: این قسمت حداقل طول عمر رمز عبور را تعیین می کند! یعنی اگر کاربری رمز عبور خود را تغییر دهد، تا n روز بعد، قادر به تغییر دادن رمز عبور خود نخواهد بود.

– **Minimum Password Length**: این قسمت، حداقل طول رمز عبور را تعیین می کند؛ مثلاً طول رمز عبور نمی تواند از ۶ حرف کمتر باشد.



– **Password Must Meet Complexity Requirements**: این قسمت تعیین می کند که نوع رمز عبور کاربر بایستی ساده یا پیچیده باشد. رمزی مانند ۱۲۳۴۵۶، یک رمز ساده و رمزی مانند abc@abc123، یک رمز پیچیده به حساب می آید. در این صفحه اگر گزینه Enabled را انتخاب کنید، سیستم کاربر را مجبور می کند که از رمز های پیچیده استفاده کند. در ویندوز سرور ۲۰۰۳، این گزینه به صورت پیش فرض **غیر فعال** و در ویندوز سرور ۲۰۰۸، این گزینه به صورت پیش فرض **فعال** است.

– **Store Passwords Using Reversible Encryption**: این قسمت تعیین می کند که سیستم رمز های عبور را به گونه ای ذخیره کند که قابل بازیابی باشد. در ویندوز سرور رمز های عبور به صورت کد شده ذخیره می شوند. اگر این گزینه را فعال کنید، سیستم رمز های عبور را به گونه ای ذخیره می کند که با داشتن رمز عبور به مقدار کد شده آن و با داشتن مقدار کد

شده، می توان به رمز عبور اصلی دسترسی داشت. اما اگر این گزینه غیرفعال کنید، فقط با داشتن رمز عبور می توان به مقدار کد شده آن دسترسی داشت؛ اما اگر مقدار کد شده را داشته باشیم، نمی توان به رمز عبور اصلی دسترسی یافت.

فصل ۲۴

Remote Desktop, Terminal Server و Remote Assistance

Remote Desktop Connections –۱–۲۴

تا قبل از به وجود آمدن شبکه های کامپیوتری، کاربران برای کارکردن با هر سیستمی، مجبور بودند که به صورت فیزیکی در محل حاضر شده و پشت سیستم مورد نظر بنشینند و با آن کار کنند. اما با به وجود آمدن شبکه های کامپیوتری، این محدودیت برطرف شد و کاربران این قابلیت را پیدا نمودند که از راه دور به یک سیستم متصل شده و با آن کار کنند؛ درست مانند اینکه به طور فیزیکی پشت آن سیستم نشسته اند. یکی از ابزارهایی که اجازه این کار را به ما می دهد، نرم افزار Remote Desktop Connection است. این نرم افزار به صورت رایگان به همراه ویندوز عرضه شده است. در ادامه این فصل به معرفی این نرم افزار می پردازیم. اما استفاده از Remote Desktop Connection یک محدودیت بزرگ دارد. و آن اینکه همزمان فقط یک کاربر می تواند با سیستم کار کند. بدین معنا که اگر کاربری با یک سیستم در حال کارکردن باشد و کاربری بخواهد از راه دور به سیستم متصل شود، کاربر جاری از سیستم خارج شده و Log out خواهد شد. مشکل دیگری که وجود دارد، مشکل عدم مدیریت کاربر متصل شده است. برای حل این مشکل، ویندوز سرور ابزار جدیدی به نام Terminal Server را معرفی نمود.

Terminal Server –۲–۲۴

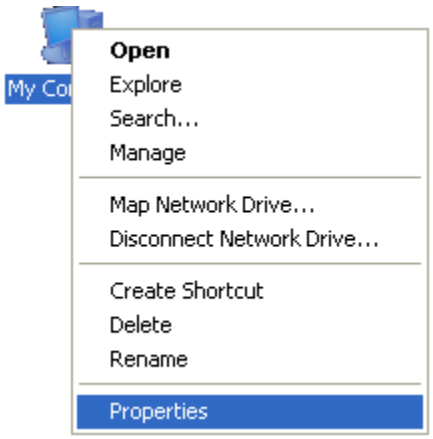
در قسمت قبل گفتیم که در ویندوز، برای اتصال به سیستم راه دور دو مشکل عمده داشتیم: ۱- وجود همزمان فقط یک کاربر ۲- عدم مدیریت کاربران وارد شده. برای حل این مشکل، ویندوز سرور ابزار جدیدی به نام Terminal Server را معرفی نمود. بدین معنا که این ابزار این قابلیت را می دهد که در یک لحظه، تعداد نا محدودی کاربر به یک سیستم Login کنند. تمام این کاربران می توانند با یک نام کاربری یا با نام های کاربری متفاوت وارد سیستم شوند و هیچ کدام از کاربران نیاز به Log out به هنگام ورود کاربر جدید ندارند. همچنین تاثیرات تغییرات دیگر کاربران به سرعت نمایان می شود. یعنی فرض کنید دو کاربر با نام کاربری Reza وارد سیستم شده باشند؛ اگر هر دو در صفحه دسکتاپ باشند، اگر یکی از کاربران فایلی را روی صفحه

دسکتاپ ایجاد کند، کاربر دوم به محض ایجاد فایل، آن را مشاهده نموده و قابلیت استفاده از آن را پیدا می کند. به علاوه توسط Terminal Server این قابلیت وجود دارد که بتوان کاربرانی که به سرور Login کرده اند را مشاهده و آن ها را مدیریت نمود.

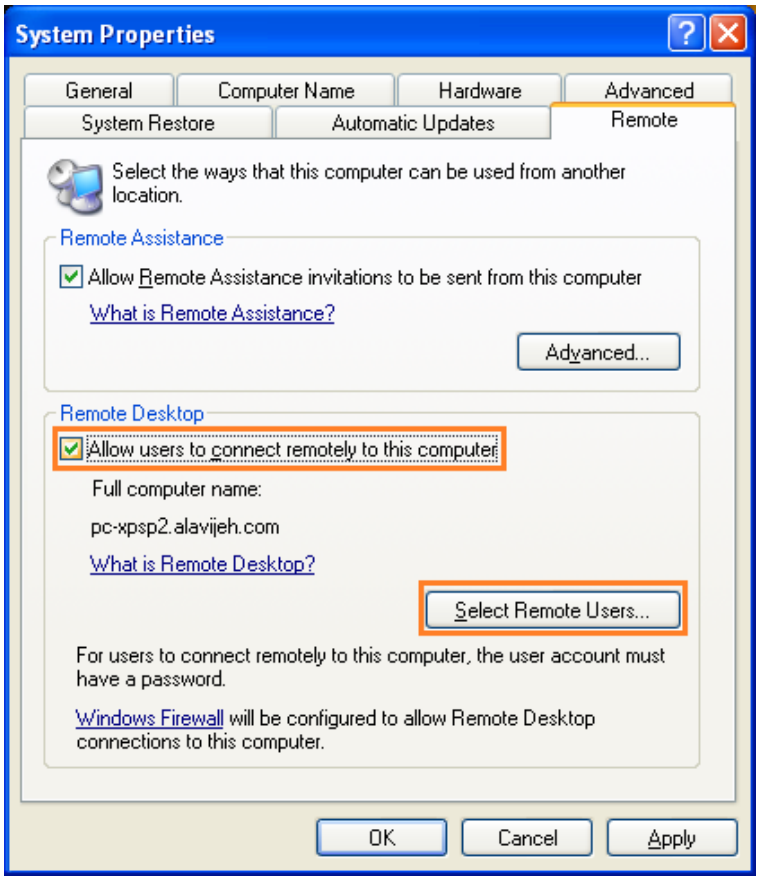
در ادامه، ابتدا به آموزش Remote Desktop Connection پرداخته و سپس به معرفی Terminal Server می پردازیم.

۲۴-۳- آماده سازی ویندوز XP جهت Remote Desktop Connection

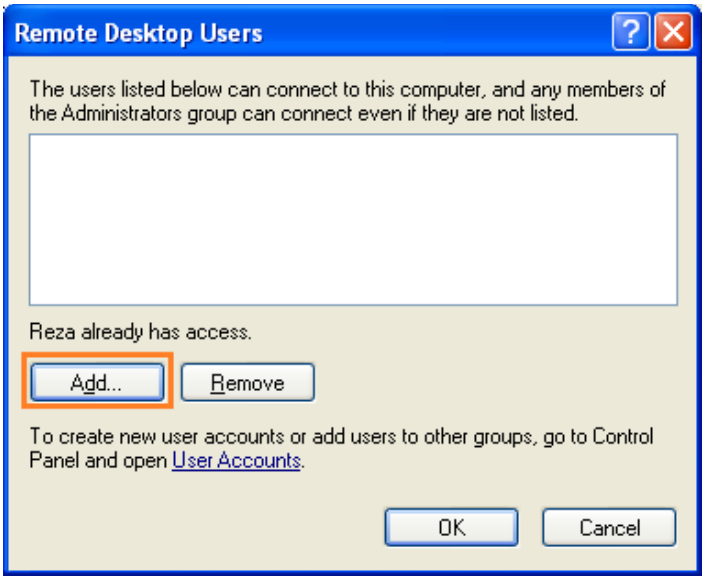
فرض کنید که قصد دارید به سیستمی متصل شوید که روی آن ویندوز XP نصب است. در این صورت مجبور هستید از Remote Desktop Connection استفاده نمایید (در مورد محدودیت های این روش در بالا صحبت کردیم). بدین منظور ابتدا بایستی تنظیماتی را در ویندوز XP انجام دهید. برای شروع، روی My Computer راست کلیک کرده و گزینه Properties را انتخاب نمایید.



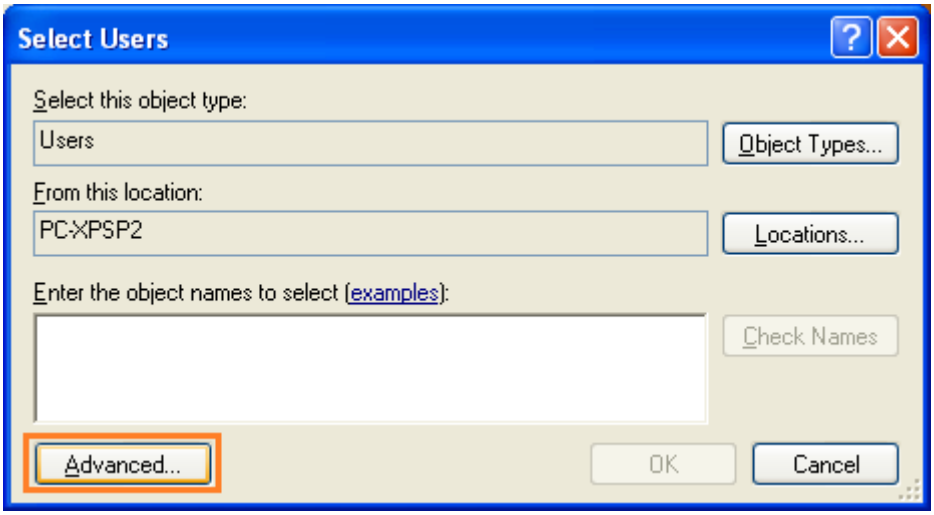
سپس در صفحه باز شده، وارد سربرگ Remote شوید. اولین کاری که باید انجام دهید، فعال کردن سرویس Remote Desktop Connection روی ویندوز است. بدین منظور، در قسمت Remote Desktop تیک گزینه Allow user to connect remotely to this computer را فعال کنید. سپس بایستی کاربرانی را مشخص کنید که اجازه Remote کردن را دارند. این بدان معنا است که هنگام ورود به سیستم راه دور، نیاز به وارد کردن نام کاربری و رمز عبور داریم. لذا باید یکی از نام های کاربری و رمز عبوری را وارد نماییم که در این قسمت مشخص شده است. به صورت پیش فرض در ویندوز XP، فقط کاربرانی اجازه ورود به سیستم به صورت Remote را دارند که عضوی از گروه Remote Desktop باشند. یعنی کاربری که تعریف کرده اید را باید عضوی از (Member of) گروه Remote Desktop کنیم. برای انجام این کار، در همین صفحه روی دکمه Select Remote Users کلیک کنید.



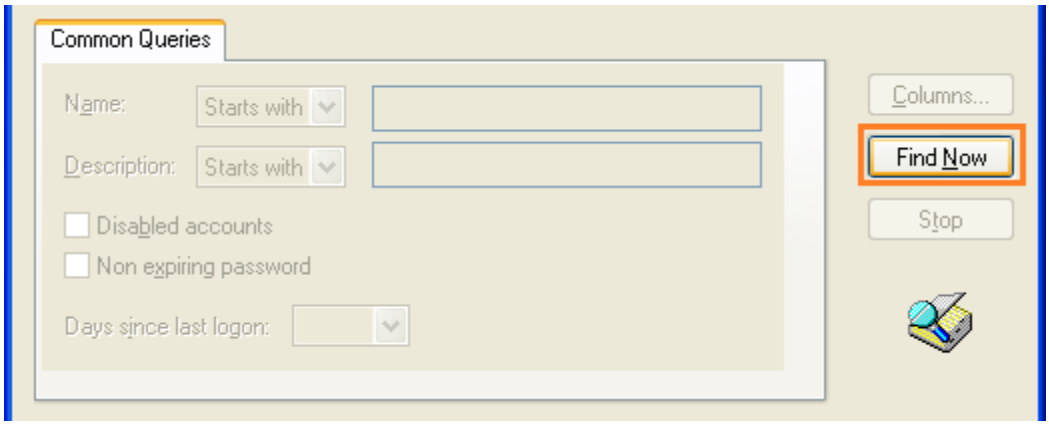
در صفحه باز شده، برای افزودن کاربر به گروه Remote Desktop، روی دکمه Add کلیک نمایید.



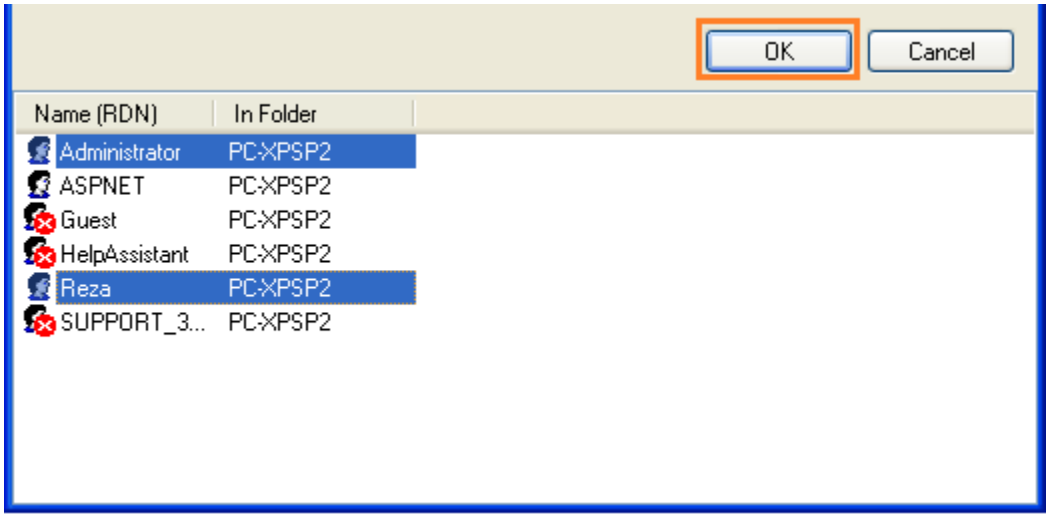
در این صفحه، دو راه برای انتخاب کاربران خود دارید. راه اول وارد کردن نام کاربر به صورت دقیق در جعبه متن پایین و سپس کلیک روی دکمه Check Names برای بررسی صحت نام وارد شده می باشد. راه دوم، انتخاب کاربر به صورت Visual (بصری) است. بدین منظور روی دکمه Advanced کلیک کنید.



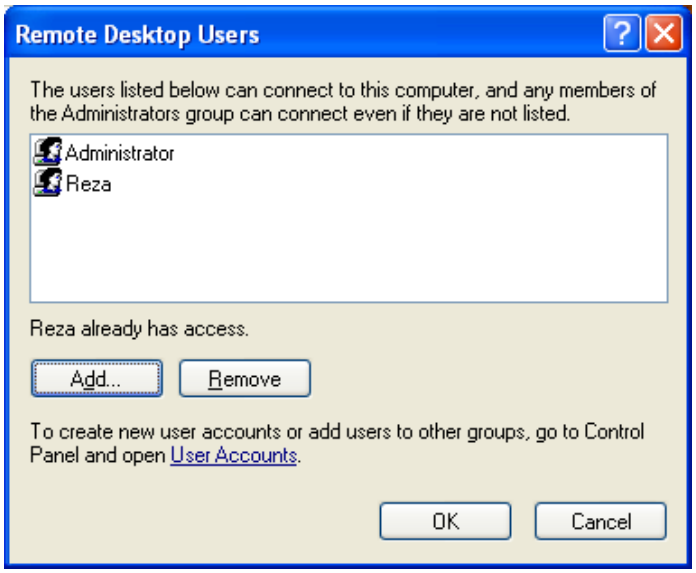
در صفحه باز شده، روی دکمه Find Now کلیک کنید تا لیست کاربران و گروه ها ظاهر شود.



سپس کاربر یا کاربران مورد نظر که قصد دارید قابلیت Remote را داشته باشند، انتخاب کرده و سپس روی دکمه OK کلیک کنید.

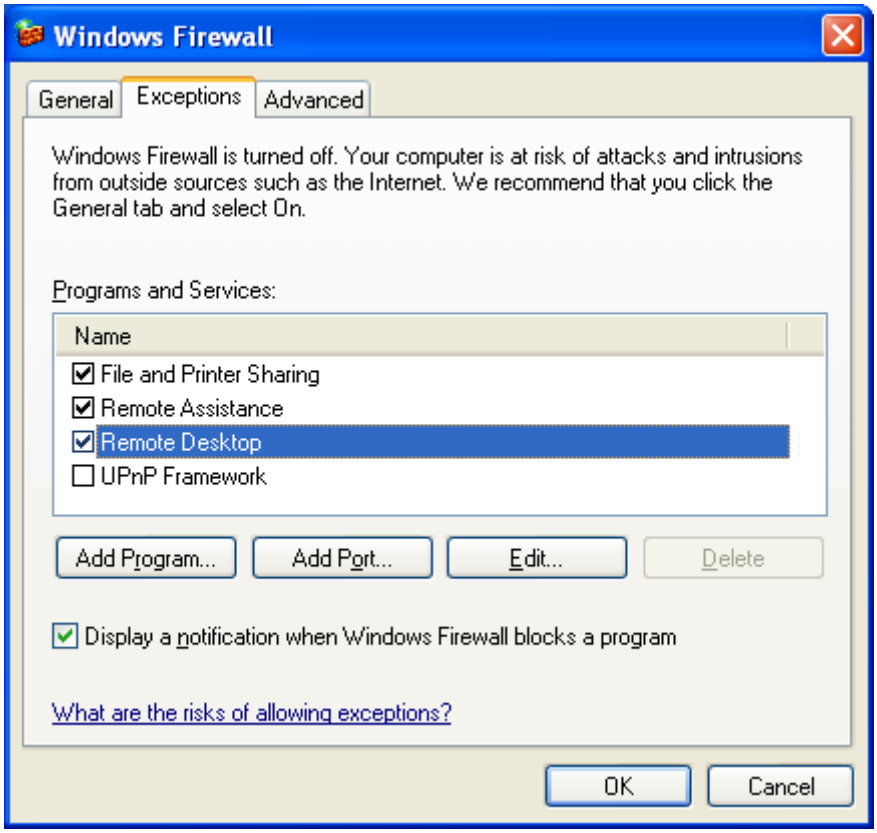


در این صفحه لیست کاربران اضافه شده را مشاهده می نمایید. در نهایت روی دکمه OK کلیک کنید.



در مرحله بعد بایستی به Firewall بگویید که اجازه دسترسی به صورت Remote را بدهد (Firewall یک ابزار امنیتی در ویندوز است). بدین منظور وارد Control Panel شده و سپس برنامه Windows Firewall را باز نمایید.

سپس در صفحه باز شده، وارد سربرگ Exceptions شده و سپس گزینه Remote Desktop را فعال نمایید. در نهایت روی دکمه OK کلیک کنید.

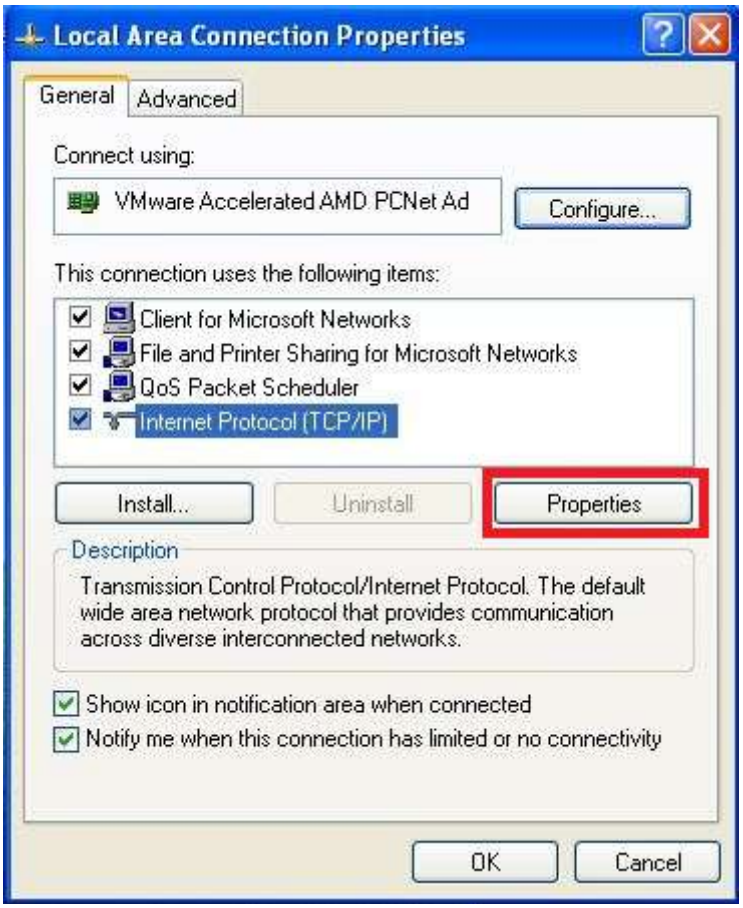


در مرحله آخر، بایستی آدرس IP کامپیوتر را تعیین نمایید. بدین دلیل که کامپیوتر ها برای اتصال راه دور از آدرس IP استفاده می کنند. البته برای اتصال، امکان استفاده از نام کامپیوتر نیز وجود دارد. برای انجام تنظیمات IP، وارد مسیر زیر شوید:

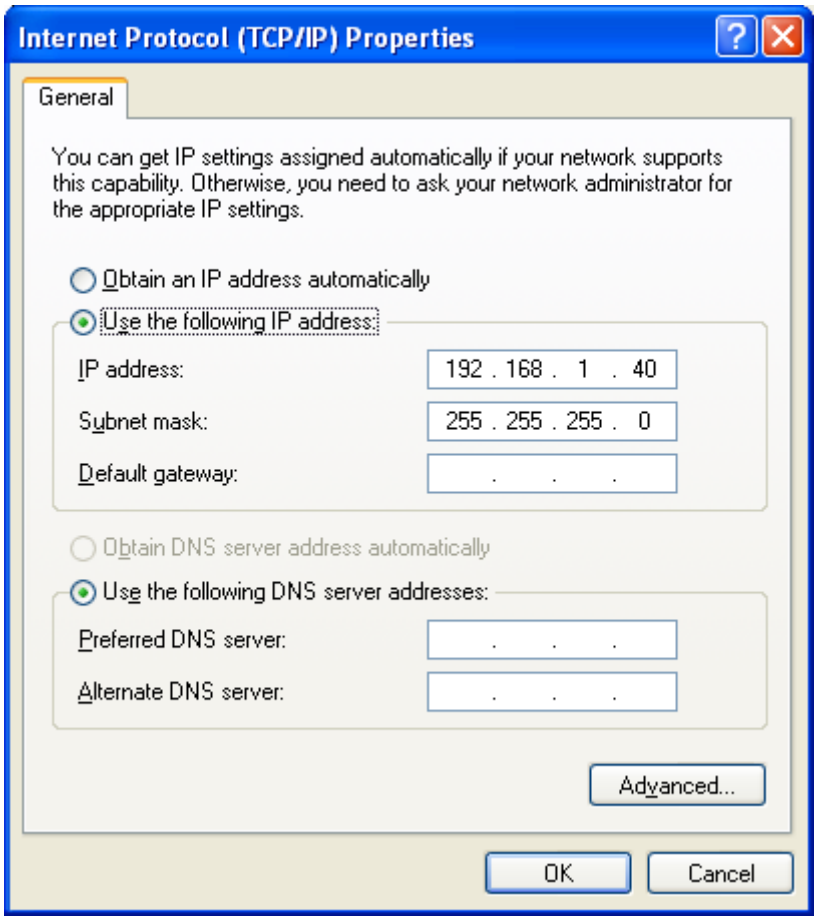
Control Panel ➔ Network Connections

روی Local Area Network راست کلیک کرده و Properties را انتخاب نمایید.

در صفحه باز شده، گزینه Internet Protocol (TCP/IP) را انتخاب کرده و سپس روی دکمه Properties کلیک نمایید.



در صفحه باز شده، مانند شکل، آدرس IP را به صورت دستی تنظیم کنید. البته نیازی به تخصیص آدرس به صورت دستی نیست. تنها چیزی که نیاز داریم، دانستن آدرس IP یا نام کامپیوتر جهت اتصال راه دور است. در نهایت روی OK کلیک کنید.



تا این مرحله، سیستم ما قابلیت پذیرش اتصال Remote را پیدا کرده است. فقط کافیست از سیستم های دیگر بـه آن متصـل شویم.

۴-۲۴- استفاده از Remote Desktop Connection در ویندوز XP

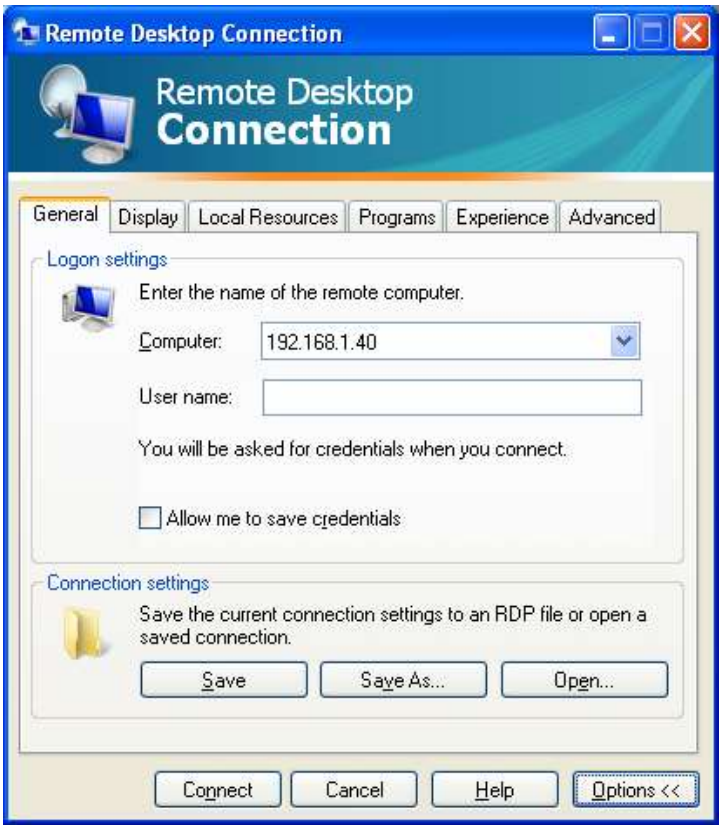
در این مرحله قصد داریم که توسط این سیستم به سیستم راه دور (سیستمی که آن را در مرحله قبل تنظیم نمودیم) متصـل شویم. برای این کار، ابتدا نرم افزار Remote Desktop Connection را اجرا نمایید. محل این نرم افزار به صورت زیر است:

Start ➔ Accessories ➔ Communications ➔ Remote Desktop Connection

پس از اجرای نرم افزار Remote Desktop Connection، صفحه ای مانند شکل زیر نمایان می شود. در این صفحه ابتدا آدرس IP یا نام کامپیوتر مقصد (Remote) را وارد نمایید. در نهایت برای اتصال، روی دکمـه Connect کلیـک کنیـد. البتـه قبـل از اتصال، می توان تنظیماتی را نیز انجام داد. بدین منظور روی دکمه Options کلیک نمایید.

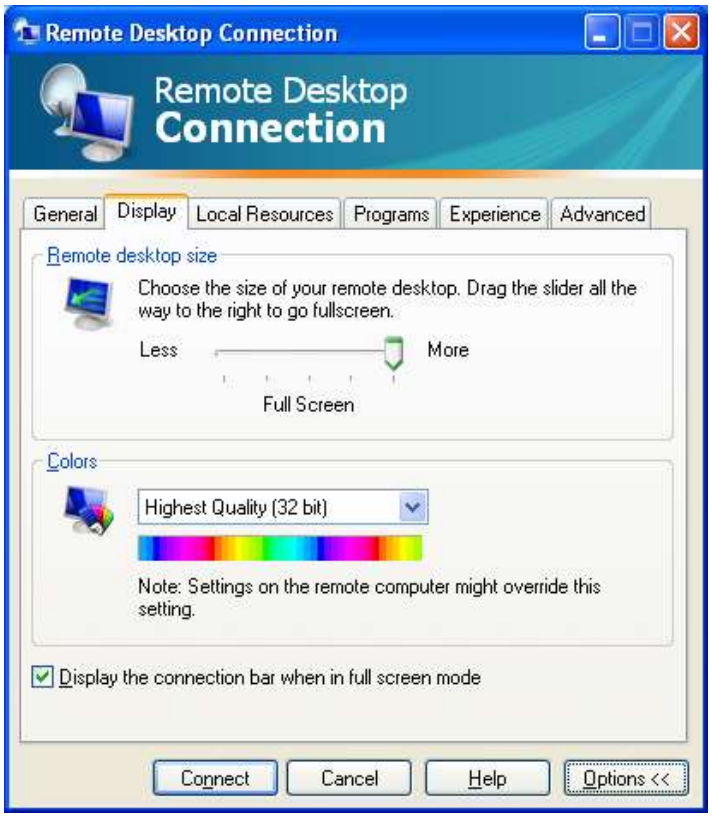
سربرگ General

در سربرگ General مربوط به تنظیمات، شما این قابلیت را دارید که نام کاربری خود جهت اتصال را وارد نمایید. البته توجه فرمایید که رمز عبور را فعلا نمی توانید وارد کنید. همچنین در این قسمت قابلیت ذخیره یا بازیابی تنظیمات وجود دارد.



سربرگ Display

در این صفحه، قابلیت تنظیم وضوح تصویر نمایشی را دارید. این امر زمانی کاربرد دارد که سرعت اتصال شما کم باشد و بخواهد مقدار اطلاعات انتقالی هنگام نمایش صفحه کامپیوتر راه دور را کاهش دهید. مثلاً تنظیم کنید که سیستم رنگ ۱۶ بیتی شده؛ یا وضوح تصویر کم شود.

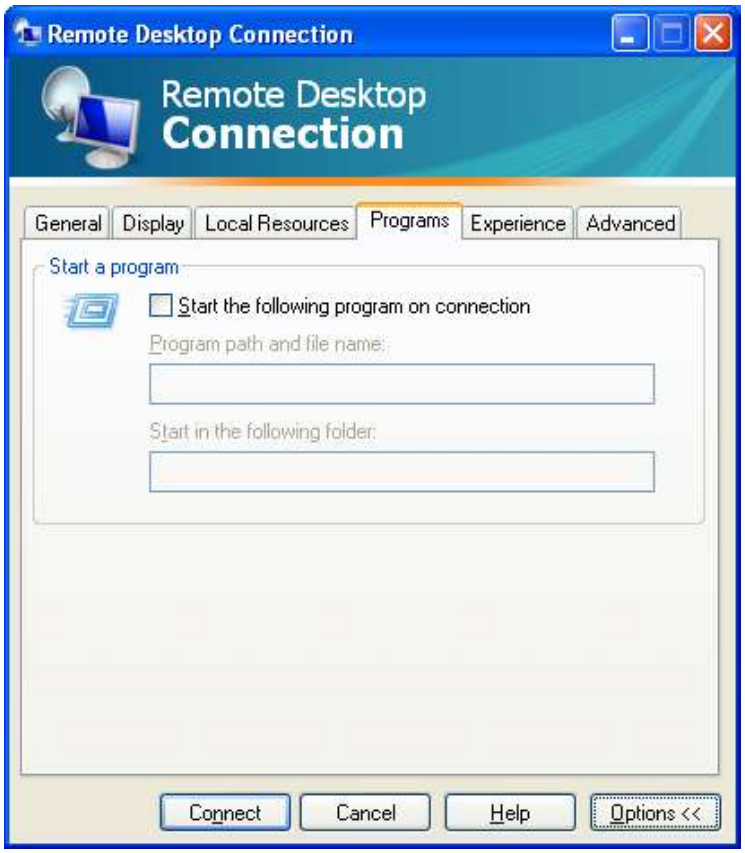


سربرگ Local Resource

در این سربرگ، می توانید تعیین کنید که قصد دارید از کدام یک از منابع کامپیوتر راه دور استفاده نمایید. مثلاً تنظیم کنید که صداهایی که روی کامپیوتر راه دور پخش می شوند را توسط Speaker خود بشنوید یا اینکه درایوهای Hard Disk کامپیوتر راه دور را در سیستم خود مشاهده نمایید.

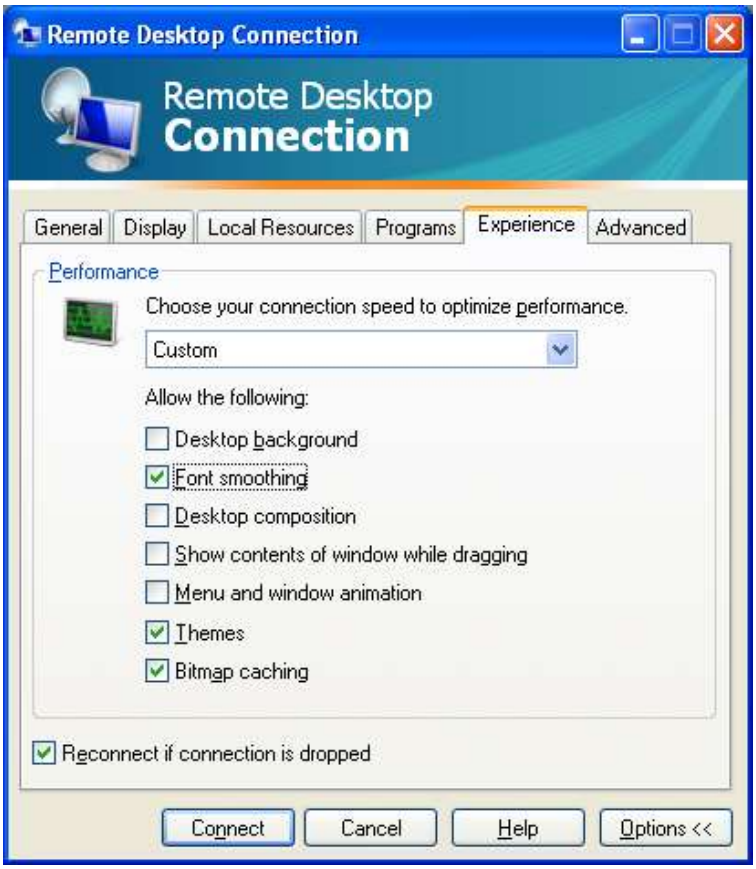
سربرگ Programs

در این قسمت می توانید تعیین کنید که در زمانی که به کامپیوتر راه دور متصل هستید، کدام برنامه اجرا شود. بدین منظور آدرس کامل برنامه و آدرس پوشه آن را وارد کنید. مثلاً برای اجرای برنامه موجود در مسیر C:\Program\Calc.exe، در جعبه متن بالایی مقدار C:\Program\Calc.exe و در جعبه متن پایینی مقدار C:\Program را وارد نمایید. منظور از جعبه متن پایینی، مقدار مسیر جاری برنامه هنگام اجرای آن است (این بحث در برنامه نویسی نمود پیدا می کند). فرض کنید که برنامه ای نوشته اید و برنامه در حال اجرا می باشد؛ شما نیز در برنامه قطعه کدی نوشته اید که مثلاً فایل A.txt را باز کند fopen("A.txt");. حال اگر مسیر جاری برنامه، همان محل وجود فایل exe باشد، فایل A.txt موجود در کنار فایل exe باز خواهد شد. اما اگر مسیر جاری برنامه را به C:\ تغییر دهیم، برنامه exe هر کجا که باشد، فایل موجود در C:\A.txt باز خواهد شد.



سربرگ Experience

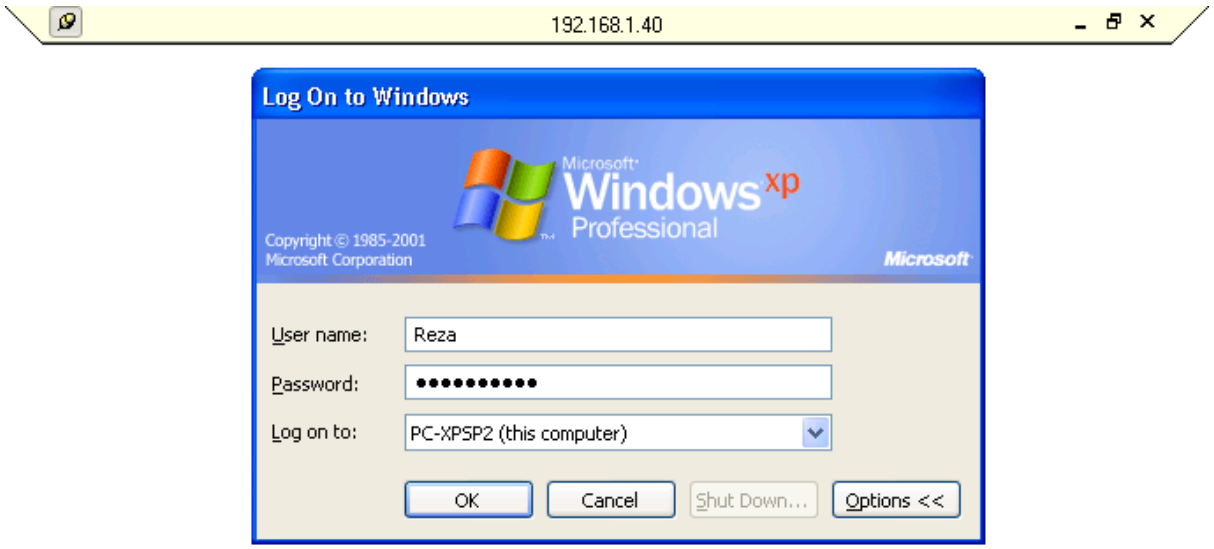
در این قسمت می توانید تنظیماتی که مربوط به کارآیی (سرعت) اتصال است را وارد نمایید. مثلاً نمایش Background یا Theme کامپیوتر راه دور. اگر سرعت اتصال شما کم است. این قسمت را تنظیم نمایید.



سربرگ Advanced

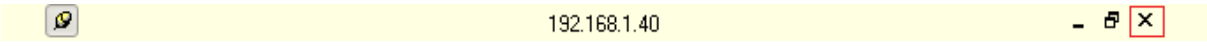
در این قسمت می توانید تنظیماتی همچون تنظیمات امنیتی را انجام دهید.

در نهایت پس از انجام تنظیمات، جهت اتصال به کامپیوتر راه دور، روی دکمه Connect کلیک کنید. اگر کامپیوتر مقصد درست پیکربندی شده باشد، صفحه Login به سیستم را مشاهده می کنید. جهت ورود به سیستم، در صفحه باز شده، نام کاربری و رمز عبور را وارد نمایید.

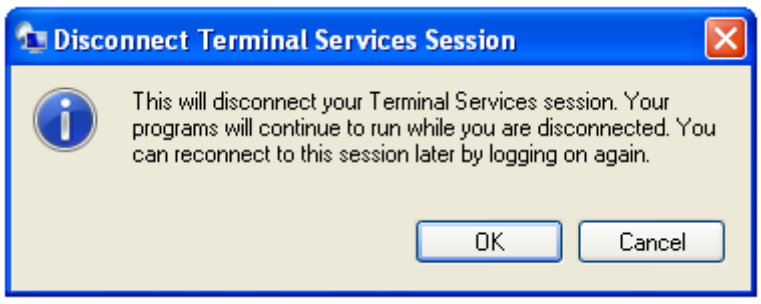


اگر نام کاربری و رمز عبور صحیح باشد، صفحه کامپیوتر مقصد را خواهید دید. گفتیم که یکی از معایب Remote Desktop Connection، این است که همزمان بیش از یک کاربر نمی تواند به یک سیستم Login کند. حال اگر به کامپیوتر راه دور سری بزنید، خواهید دید که کاربر آن Log out شده است. البته در عمل، کاربر Lock شده و اجازه کار ندارد. در صورت Unlock کردن، کاربر راه دور خارج خواهد شد.

برای قطع اتصال خود، روی دکمه Close که در بالای صفحه موجود است، کلیک نمایید.



قبل از بسته شدن، سیستم اخطار می دهد که با بستن صفحه Session شما قطع نشده و بعدا می توانید مجددا به سیستم Login کنید و کا خود را تا جایی که پیش رفته است؛ ادامه دهید.

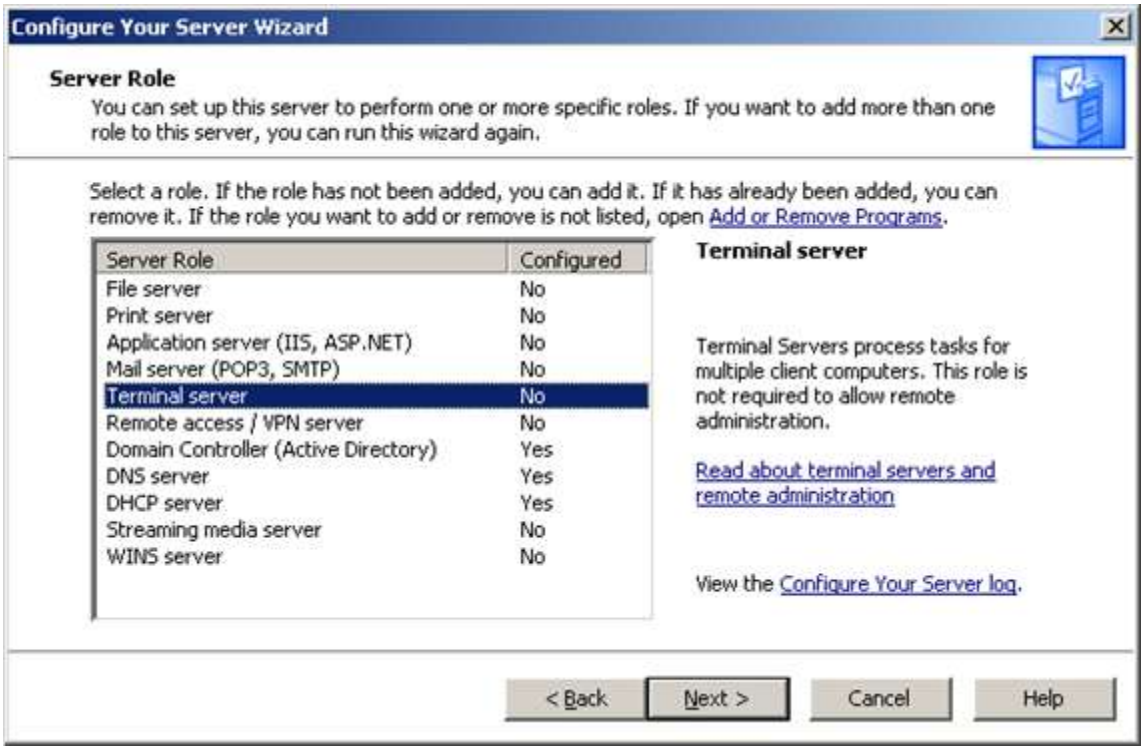


۵-۲۴- راه اندازی Terminal Server در ویندوز سرور

در بخش های فوق با مشکلات Remote Desktop Connection آشنا شدید. برای حل این مشکلات، مایکروسافت Terminal Server را معرفی کرد. برای استفاده از این سرویس، بایستی ابتدا آن را روی ویندوز سرور نصب کنید. بدین منظور، مسیر زیر را اجرا کنید: Start ➔ Administrative Tools ➔ Configure Your Server Wizard. این بخش جهت افزودن نقش (Role) به سرور مورد استفاده قرار می گیرد.

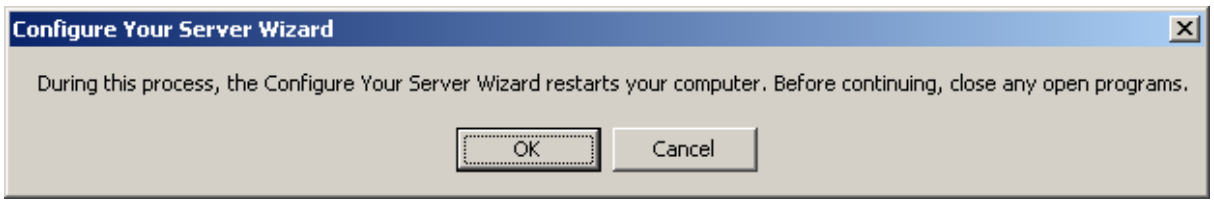
ابتدا صفحه خوش آمد گویی باز می شود. در این صفحه ، دکمه Next را بزنید.

در صفحه باز شده، گزینه Terminal Server را انتخاب کنید، این بدان معناست که می خواهید نقش Terminal Server را به این کامپیوتر بدهید. سپس روی دکمه Next کلیک کنید.

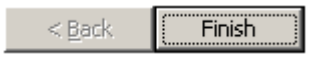


مجددا روی دکمه Next کلیک کنید.

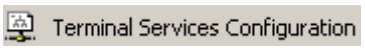
در این صفحه، سیستم به شما پیغام می دهد که پس از نصب Terminal Server، سیستم شما Restart خواهد شد. لذا تمامی برنامه های باز شده را ببندید.



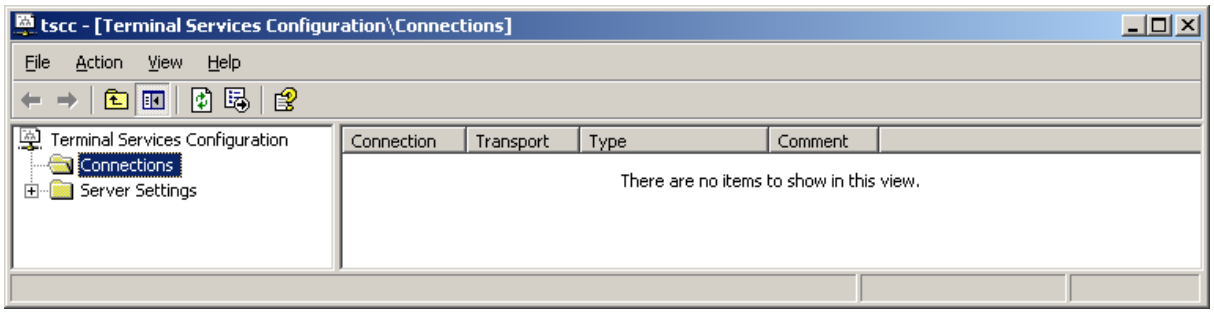
صبر کنید تا سیستم، Terminal Server را نصب کند. در صورتی که سیستم از شما سی دی ویندوز سرور را خواست، آن را در دستگاه قرار دهید. پس از پایان نصب، روی دکمه Finish کلیک نمایید.



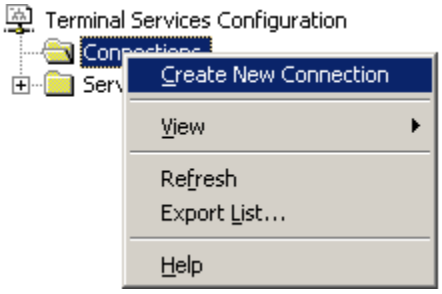
برای راه اندازی و پیکربندی Terminal Server، از مسیر Start ➔ Administrative Tools، برنامه Terminal Server Configuration را اجرا نمایید.



با اجرای برنامه Terminal Server Configuration، صفحه زیر نمایان می شود. در این صفحه می توانید اطلاعات مربوط به دریافت اتصالات راه دور را تنظیم نمایید.

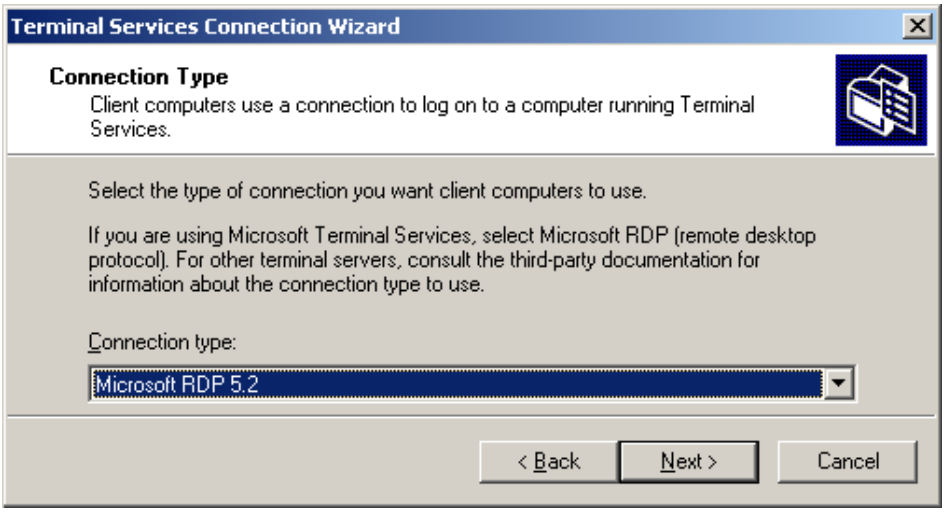


در ابتدا بایستی یک Connection جدید بسازید. این Connection مسئول پذیرش درخواست ها و اتصالات Remote خواهد بود. بدون این Connection، کاربران قادر به اتصال به ویندوز سرور نیستند. جهت ساخت Connection جدید، روی قسمت Connections راست کلیک کرده و سپس گزینه Create New Connection را انتخاب نمایید.

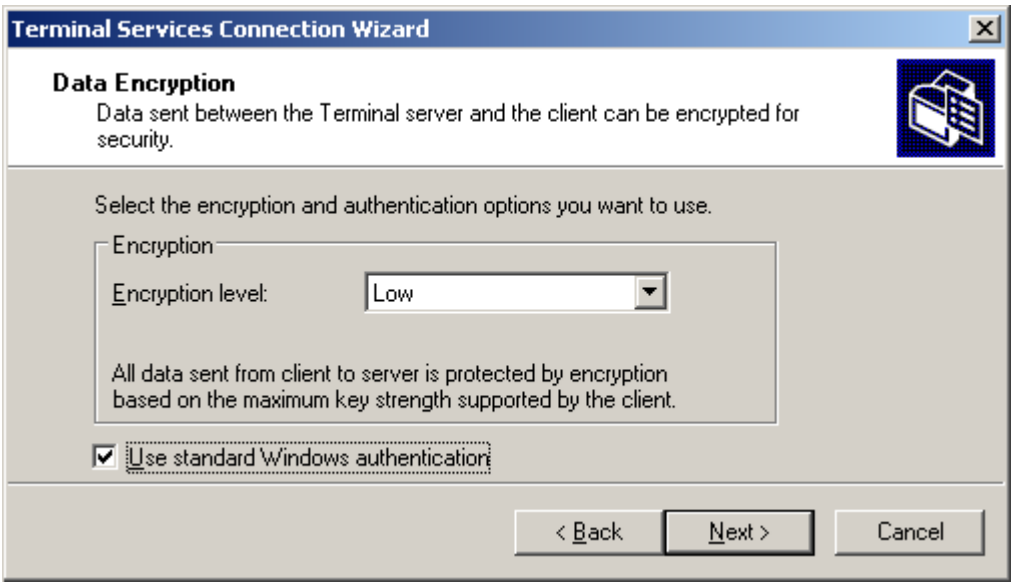


در صفحه خوش آمد گویی، روی دکمه Next کلیک کنید.

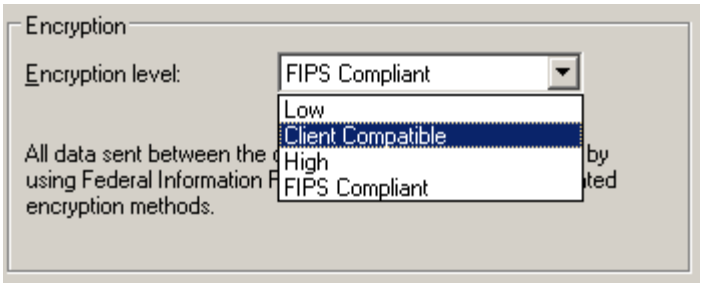
در صفحه بعد، نوع پروتکلی که برای اتصال راه دور استفاده می نمایید را انتخاب نمایید. به طور پیش فرض گزینه Microsoft RDP 5.2 انتخاب شده است. این گزینه پروتکل Remote Desktop Protocol است که توسط مایکروسافت عرضه شده است. لزوم این پروتکل، هماهنگی و توافق دستگاه ها روی اطلاعات ارسالی بین دو کامپیوتر است. سپس روی Next کلیک کنید.



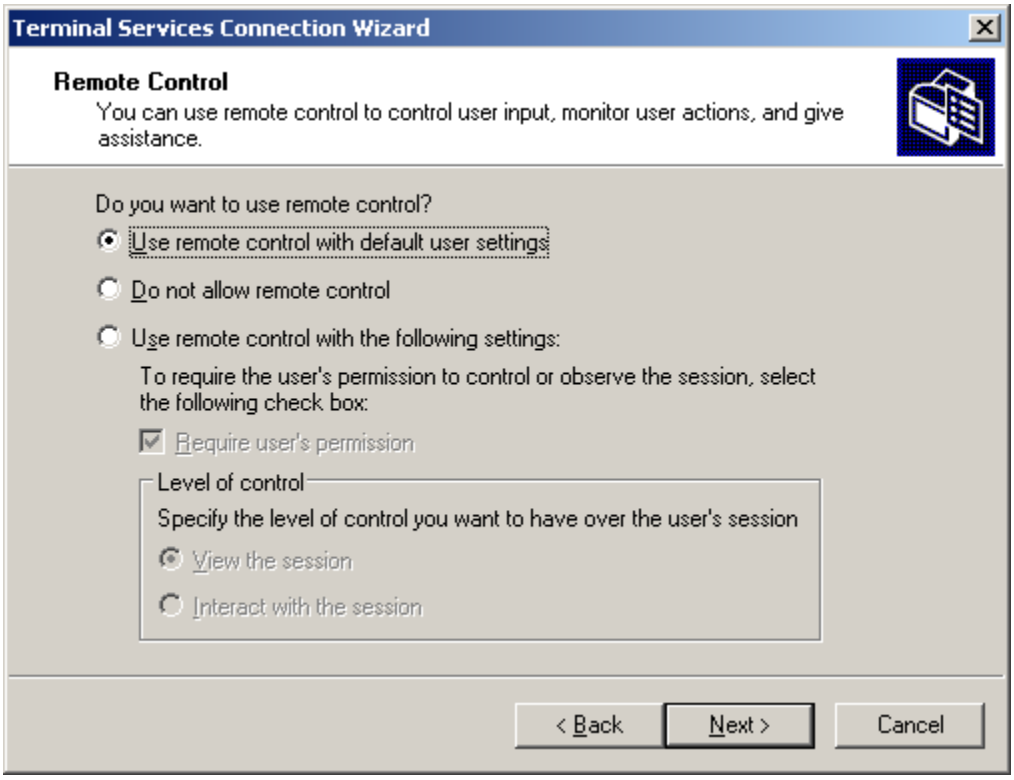
در مرحله بعد، مرحله و سطح کد گذاری (Encryption) را انتخاب کنید. در قسمت زیرین نیز گزینه Use standard Windows authentication را انتخاب نمایید تا احراز هویت کاربران ورودی توسط اعتبار سنجی ویندوز انجام شود.



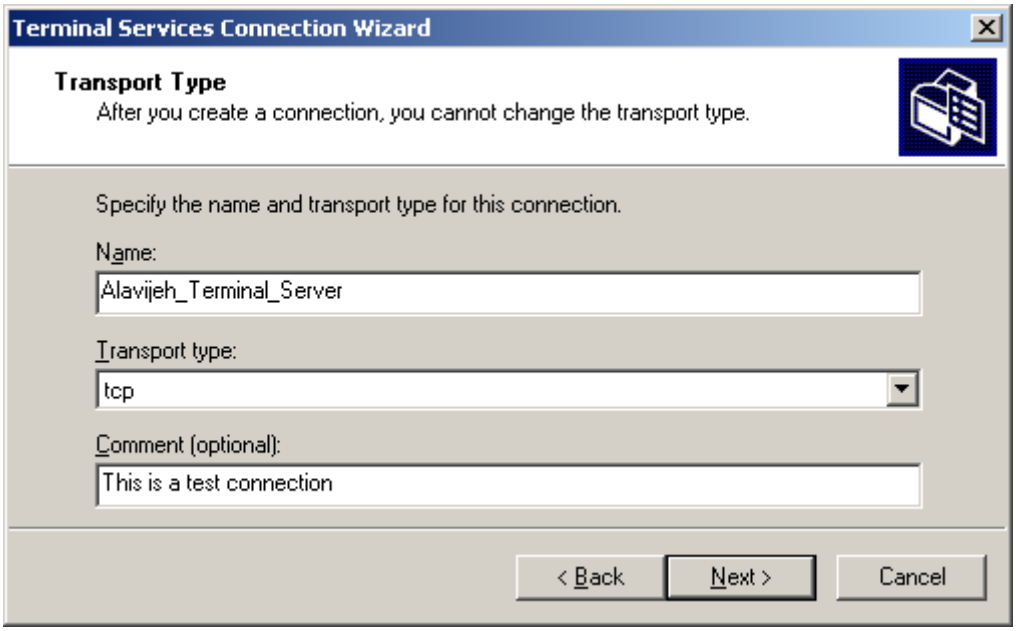
در این صفحه می توانید سطوح مختلفی از کد گذاری را انتخاب نمایید. همانطور که می دانید، هنگام کد گذاری اطلاعات یک کلید نیز برای آن تولید می شود، و عمل کد گشایی توسط این کلید انجام می شود. هرچه طول این کلید بیشتر باشد، امنیت کد گذاری بیشتر خواهد بود. اگر در این صفحه نوع Low را انتخاب کنید، طول کلید ۵۶ بیت و اگر نوع High را انتخاب کنید، طول کلید ۱۲۸ بیت خواهد بود. با انتخاب گزینه Client Compatible، طول کلید برابر با بیشترین طول قابل پشتیبانی توسط Client خواهد بود. توجه نمایید که هرچه سطح امنیت بالاتر باشد، سرعت پایین تر خواهد آمد. لذا بین امنیت و سرعت، بایستی تا حد امکان یک حد تعادل (Trade Off) قرار دهید.



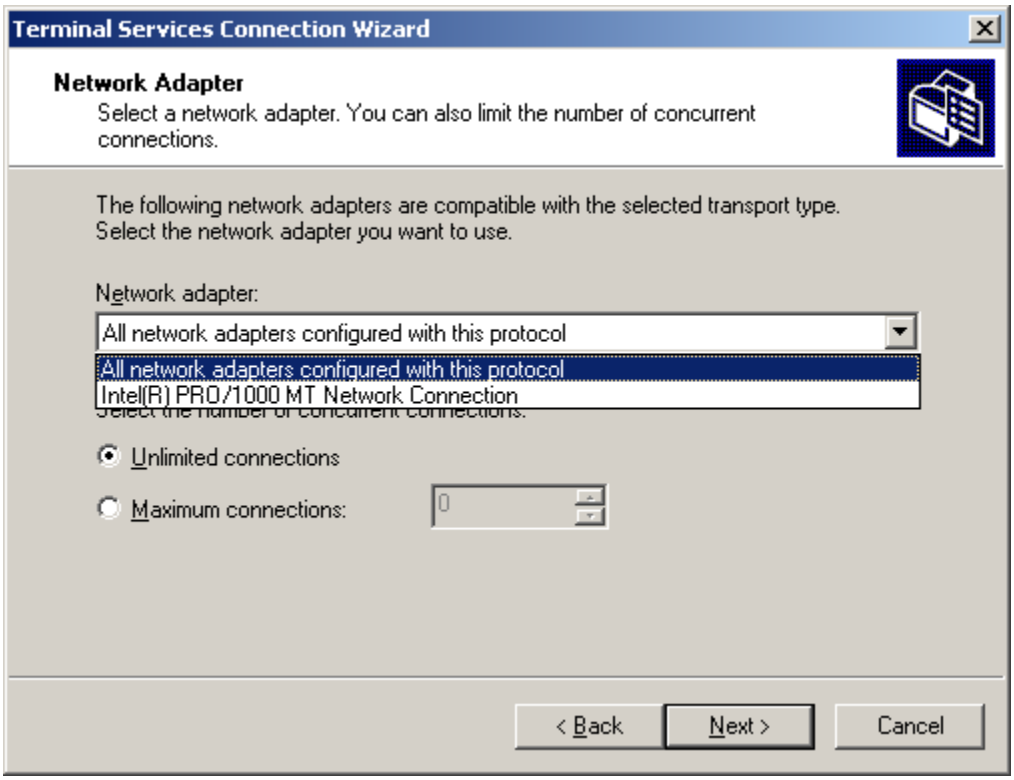
در این صفحه می توانید تنظیماتی را در مورد عدم پذیرش یا نحوه پذیرش Remote Control تعیین نمایید.



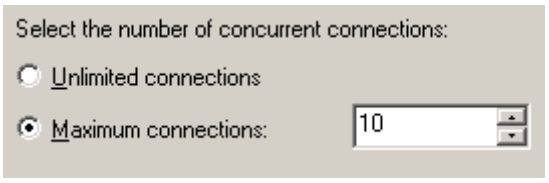
در صفحه بعد، یک نام و توصیف برای Connection خود انتخاب نمایید. همچنین می توانید نوع پروتکل انتقال را انتخاب نمایید. به صورت پیش فرض گزینه TCP فعال شود. به طور مختصر بدانید که پروتکل TCP یک پروتکل اتصال گرا و امن است. بدین معنا که با ارسال یک پیام، صبر می کند تا مطمئن شود که پیام حتما به دست مقصد می رسد. در مقابل TCP، پروتکل UDP قرار دارد. برعکس پروتکل TCP، این پروتکل امن نیست، یعنی تضمین نمی کند که پیام ارسالی حتما توسط مقصد دریافت شود؛ اما این پروتکل سرعت بالایی دارد. در نهایت روی Next کلیک کنید.



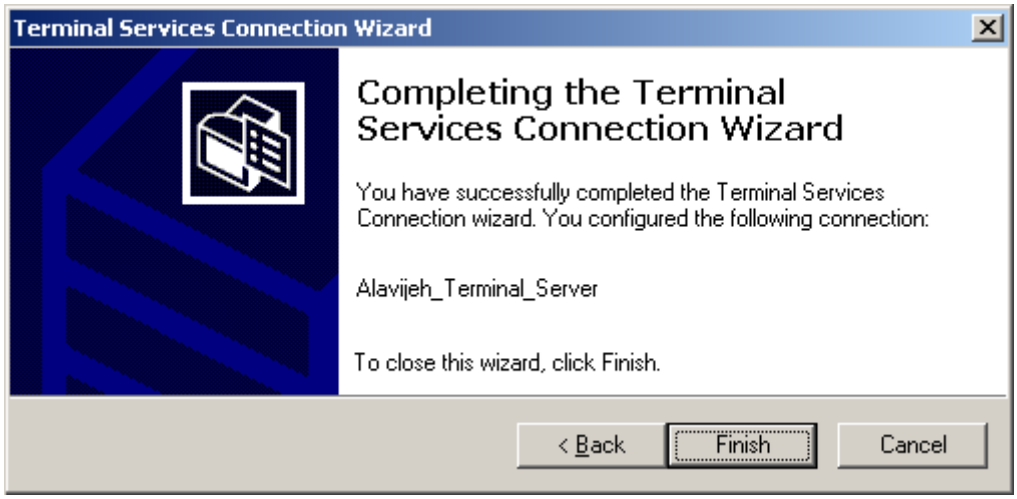
در این مرحله می توانید دو دسته تنظیمات را انجام دهید. دسته اول تعیین این موضوع است که کدام یک از تجهیزات شبکه شما (کارت شبکه، مودم و...)، مسئول رسیدگی به درخواست ها و اتصالات Remote می باشد؟ اگر گزینه اول، یعنی All network adapters configured with this protocol را انتخاب کنید، تمام تجهیزاتی که پروتکل تعیین شده در صفحه قبل را پشتیبانی می کنند، مسئول رسیدگی و مدیریت عملیات Remote خواهند بود.



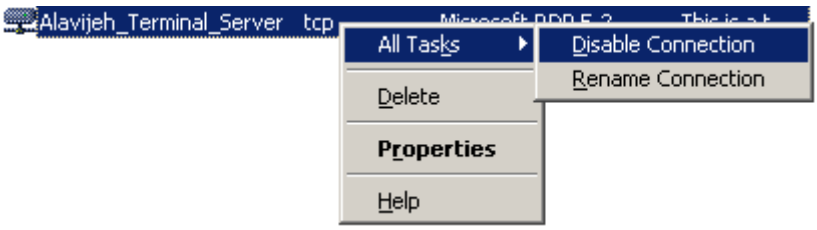
تنظیم بعدی که در این صفحه می توانید انجام دهید، این است که شما می توانید سیستم را محدود کنید که همزمان بیشتر از n کاربر، به سیستم متصل نشوند. تعیین این مقدار برای جلوگیری از شلوغی بیش از حد سرور هنگام اتصال همزمان سودمند است. در شکل زیر، ما این تعداد را به ۱۰ نفر محدود کرده ایم.



این صفحه نیز بیانگر اتمام ساخت Connection دریافت کننده اتصالات Remote است.

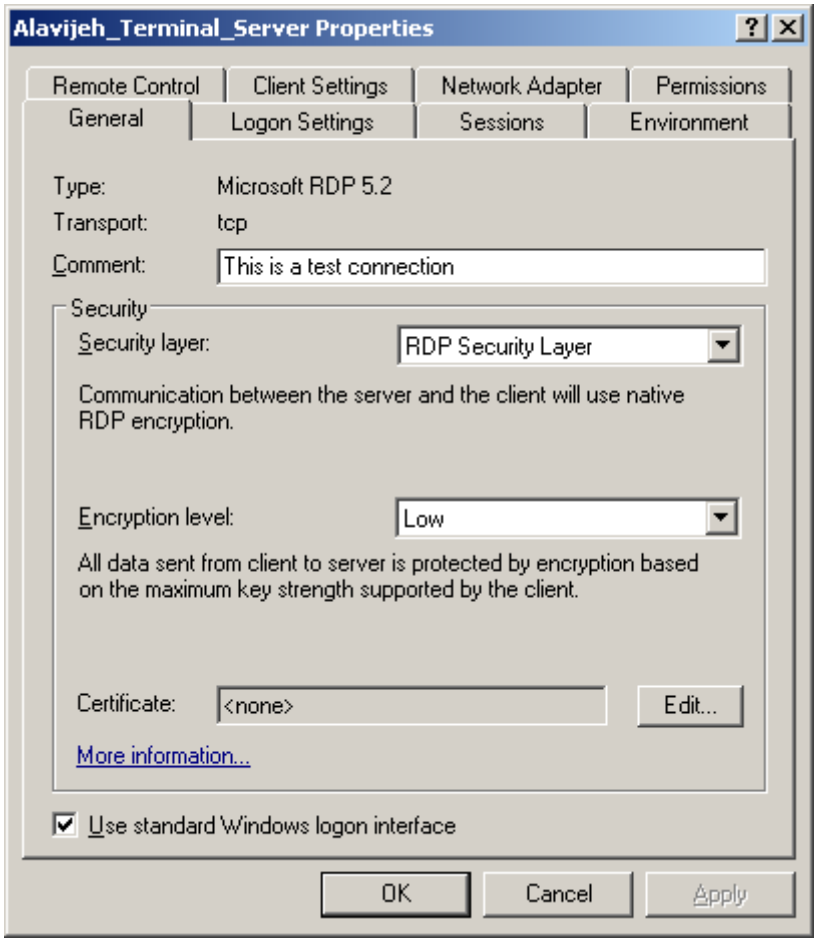


پس از ساخت Connection، ممکن است بخواهید آن را غیر فعال کنید، بدین منظور روی آن راست کلیک کرده و از قسمت All Tasks گزینه Disable Connection را انتخاب نمایید. همچنین جهت انجام تنظیمات، روی Connection ساخته شده راست کلیک کرده و گزینه Properties را انتخاب نمایید. در ادامه به معرفی قسمت های مختلف Properties می پردازیم.



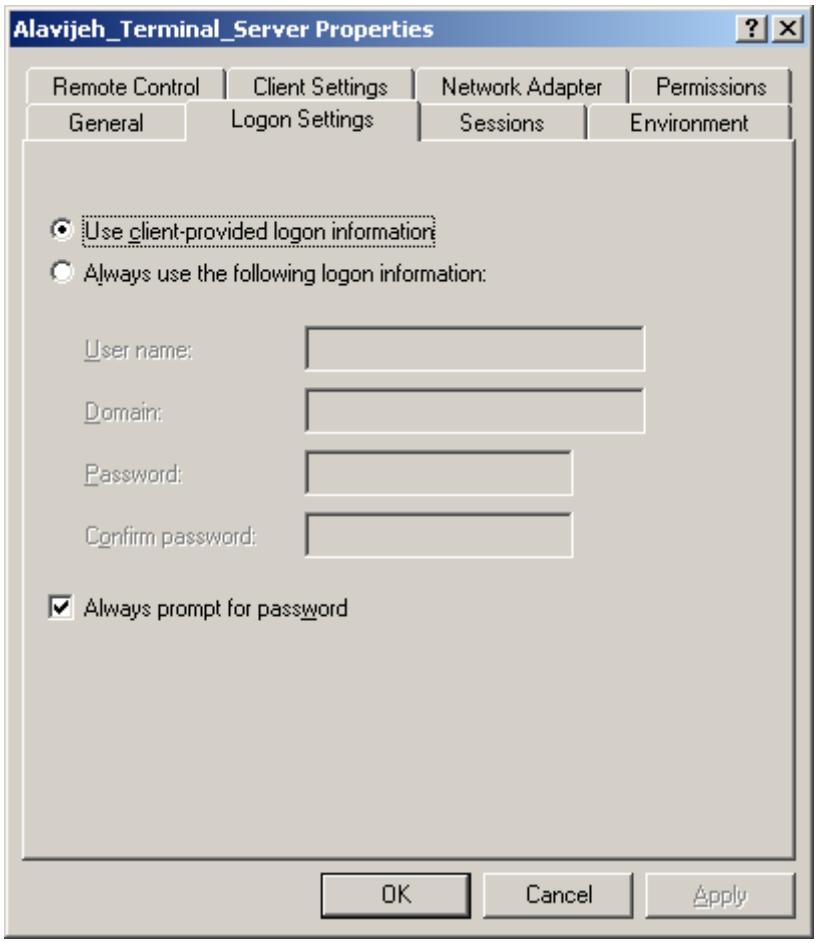
سربرگ General

در این قسمت می توانید تنظیمات اصلی نظیر لایه امنیتی، سطح Encryption، و نیز نوع احراز هویت را تعیین نمایید.



سربرگ Logon Settings

در این صفحه گزینه Use client provided logon information تعیین می کند که کاربر هنگام Login، می تواند هر User Name و Passwordی را وارد نماید و احراز هویت بر اساس User Name و Password وارد شده انجام می گیرد. اما اگر گزینه Always use the following logon information را فعال کرده و سپس مقداری را در User Name و Domain وارد نمایید، هنگام ورود کاربر، به صورت پیش فرض، همین مقادیر در صفحه Login به نمایش در خواهد آمد. همچنین اگر Always prompt for password را فعال کرده و رمزی را وارد نمایید، هنگام ورود کاربر از راه دور، به صورت خودکار همین نام کاربری و رمز عبور اعمال خواهد شد. حال اگر نام کاربری و رمز عبور آن صحیح باشد، کاربر به صورت خودکار و بدون نیاز به رمز عبور به سیستم وارد خواهد شد.



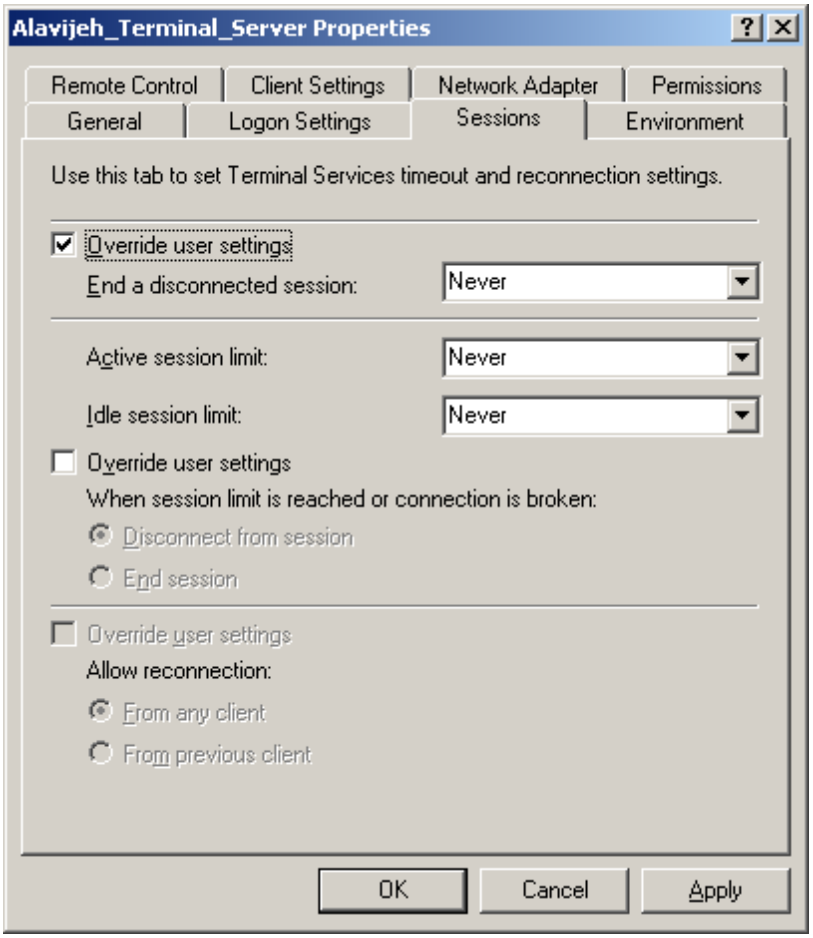
سربرگ Session

منظور از Session، اطلاعاتی در مورد جلسه ایجاد شده بین دو کامپیوتر است. در این صفحه می توانید اطلاعـاتی را در مـورد Session تنظیم نمایید. به ۳ مورد قابل تنظیم زیر توجه فرمایید:

۱. **End A Disconnected Session:** به طور پیش فرض، پس از قطع اتصال کلاینت به سرور، اطلاعات Session از بین نمی رود. به عنوان مثال، اگر کاربر به صورت Remote برنامه ای را اجرا کرده (فرض کنیـد برنامـه رایـت سـی دی) و سپس از Remote خارج شود، در این صورت برنامه قطع نشده و به کار خود ادامه می دهد (به ادامه رایت می پردازد). و کاربر با Login بعدی، می تواند ادامه کار برنامه ها را ببیند. از طریـق قسـمت End a disconnected session مـی توان تنظیم کرد که چند دقیقه پس از Log out کردن کاربر راه دور، Session از بین برود.

۲. **Active SESSION LIMIT:** از طریق این بخش می توان تنظیم کرد که کـاربر پـس از ورود بـه صـورت Remote، نهایتا تا چه زمانی می تواند داخل سیستم بماند. پس از آن به صورت خودکار، Log out خواهد شد.

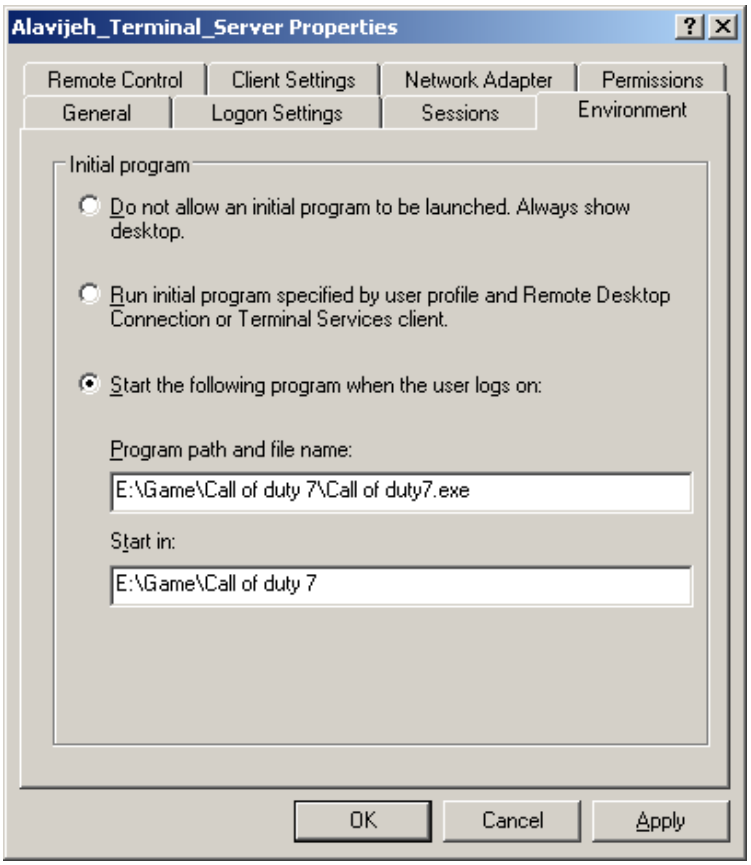
۳. **Idle Session Limit:** به کمک این قسمت می توان تنظیم کرد که کاربر تا چه زمانی می تواند بیکار باشد. منظور از بیکاری، عدم تکان دادن موس یا فشردن کلید های کیبرد است. با این تنظیم مشخص می کنیم که اگر کاربر تا زمان خاصی، از موس و کیبرد استفاده نکرد، به صورت خودکار Log out کند.



سربرگ Environment

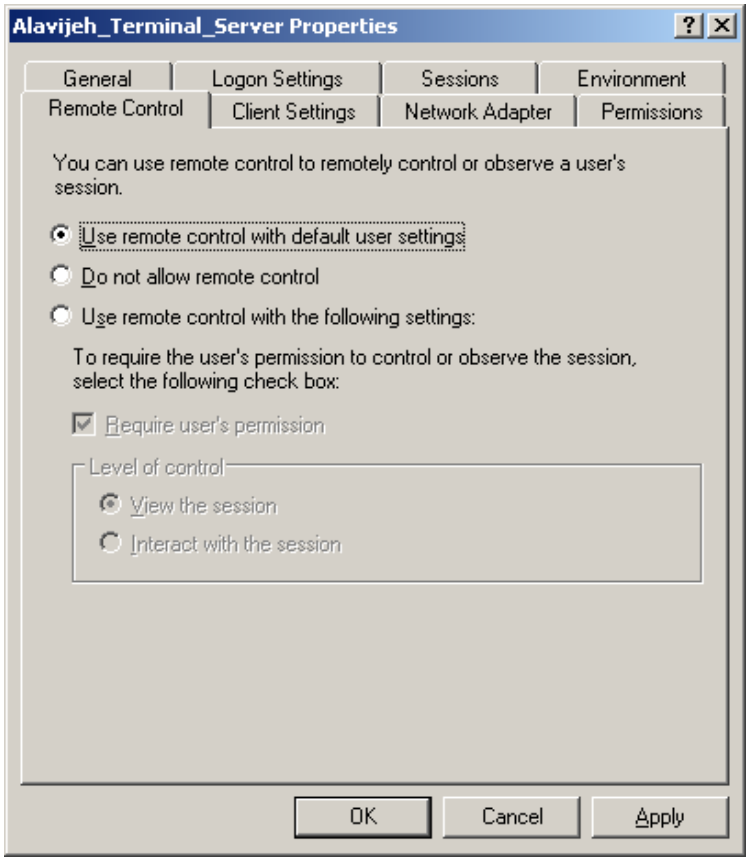
از طریق این قسمت می توان مشخص کرد که با Login کردن کاربر از راه دور، برنامه خاصی اجرا شود. قسمت های Program path and file name و Start in را به صورت زیر می توانید وارد نمایید (Start in همان Program path and file name ولی بدون نام فایل اجرایی است). لزوم وجود Start in را در بالاتر توضیح داده ایم.

توجه نمایید که با بستن برنامه، Session نیز بسته شده و کلاینت به صورت خودکار Log out خواهد شد.



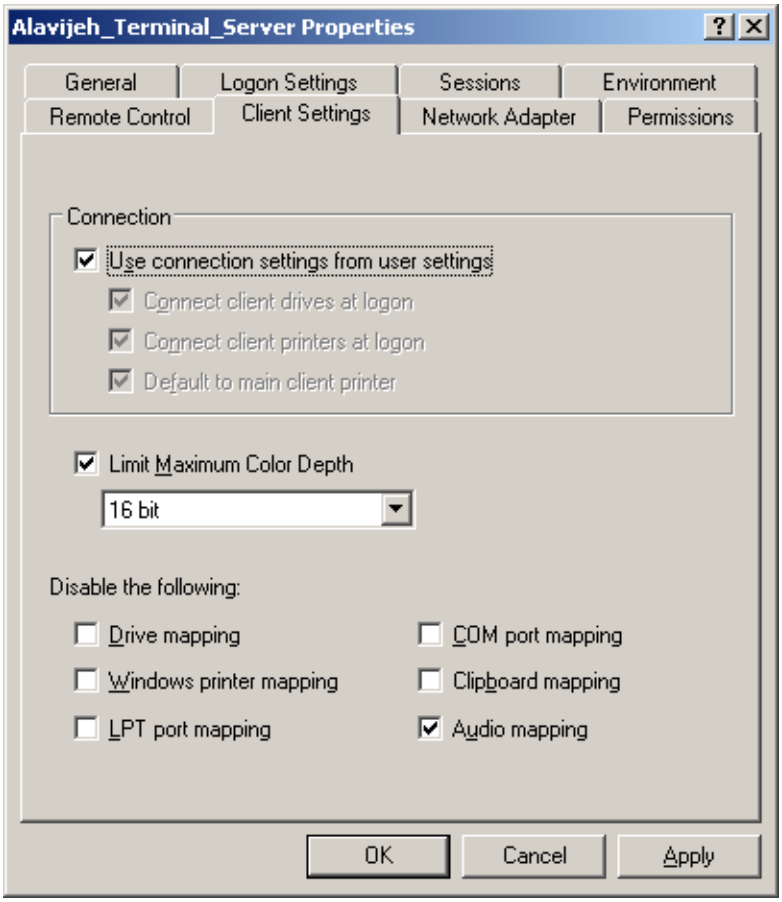
سربرگ Remote Control

در این صفحه می توانید تنظیماتی را در مورد عدم پذیرش یا نحوه پذیرش Remote Control تعیین نمایید.



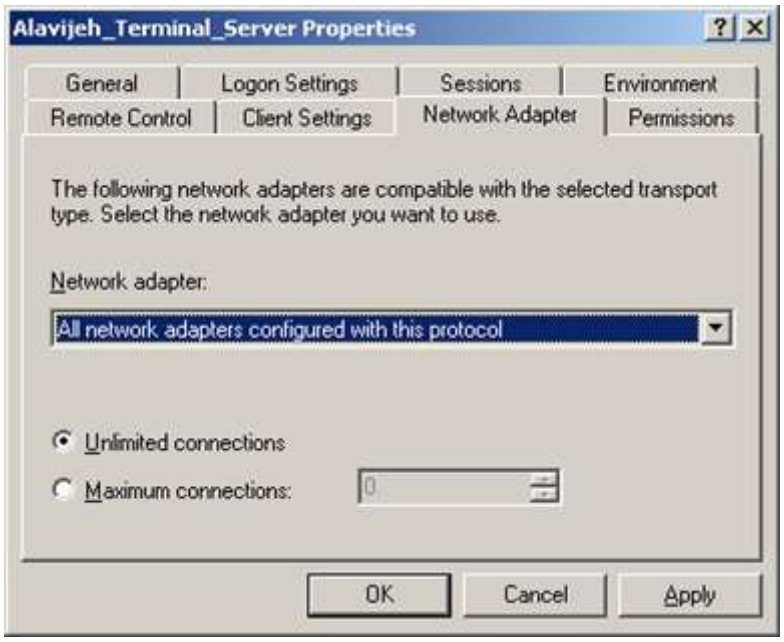
سربرگ Client Setting

در این صفحه می توان اطلاعات ارسال شده توسط Client به Server، مانند درایو ها، چاپگر، وضوح تصویر و پورت های به کار گرفته شده توسط سخت افزارهای مختلف Client را فیلتر و انتخاب نمود.



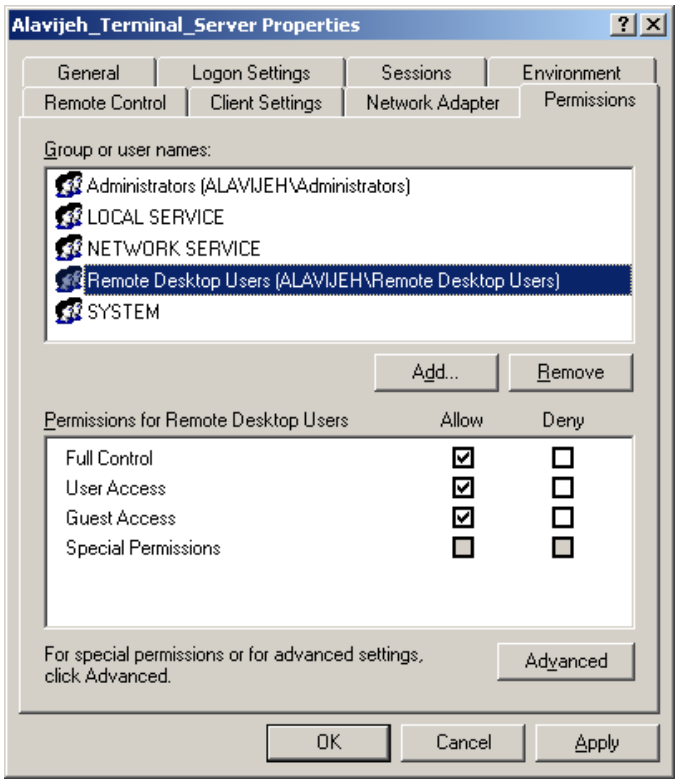
سربرگ Network Adapter

از طریق این صفحه می توان کارت شبکه دریافت کننده اطلاعات Remote، و نیز تعداد کاربرانی که به صورت همزمان قابلیت Login به سیستم را دارند را تعیین نمود.

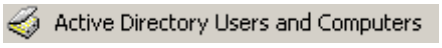


سربرگ Permissions

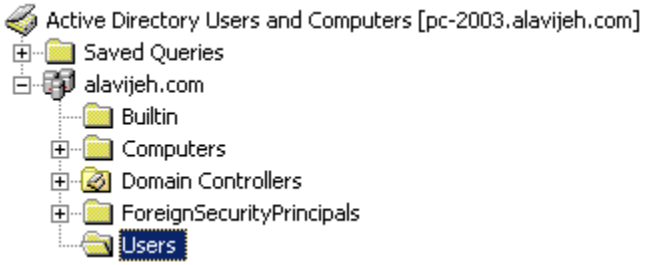
از طریق این صفحه می توانید مجوزهای لازم برای اتصال را تعیین نمایید.



تا این مرحله، شما تنظیمات لازم برای ساخت Connection را انجام داده اید. این Connection وظیفه دریافت و مدیریت عملیات Remote را دارد. اما این مراحل کافی نیست. شما نیاز دارید کاربرانی را تعیین نمایید تا توسط آن ها به صورت Remote به سیستم Login کنید. **نکته** مهم این است که فقط کاربرانی حق ورود به صورت Login دارند که عضو دو گروه **Remote Desktop** و **Domain Admins** باشند. بنابراین بایستی کاربر مورد نظر را به گروه های فوق اضافه کنید. بدین منظور از مسیر Administrative Tools ➔ Start، گزینه Active Directory Users and Computers را انتخاب نمایید.

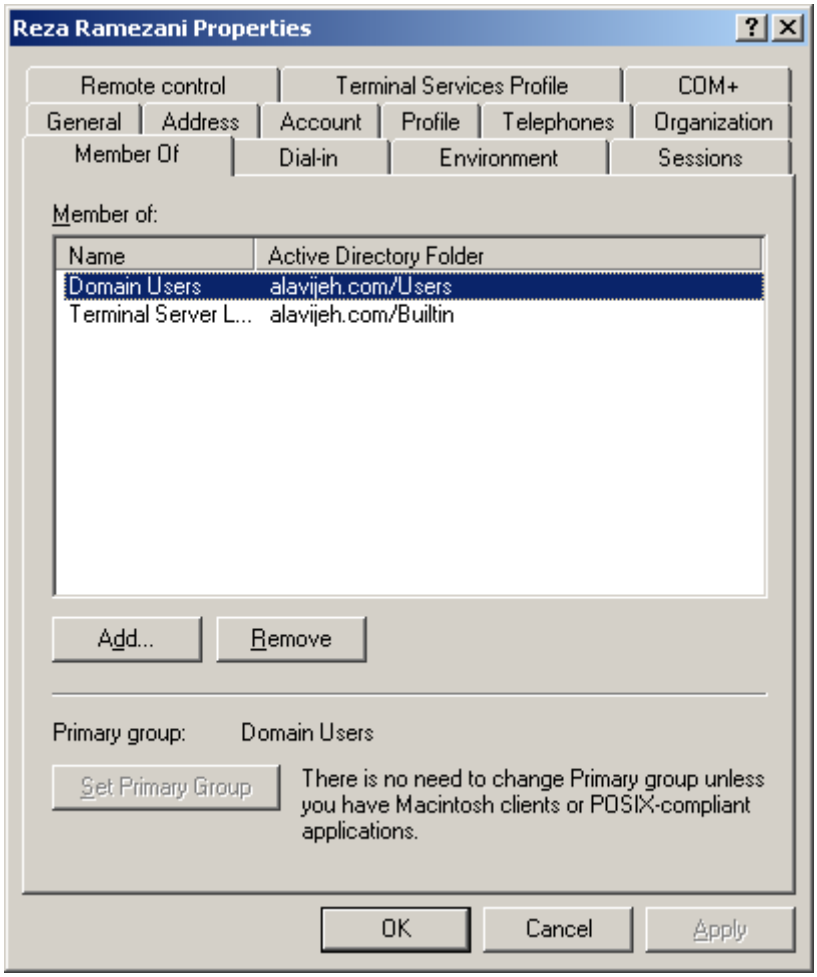


در این صفحه، روی قسمت Users کلیک کنید تا لیست کاربران و گروه های موجود را ببینید.

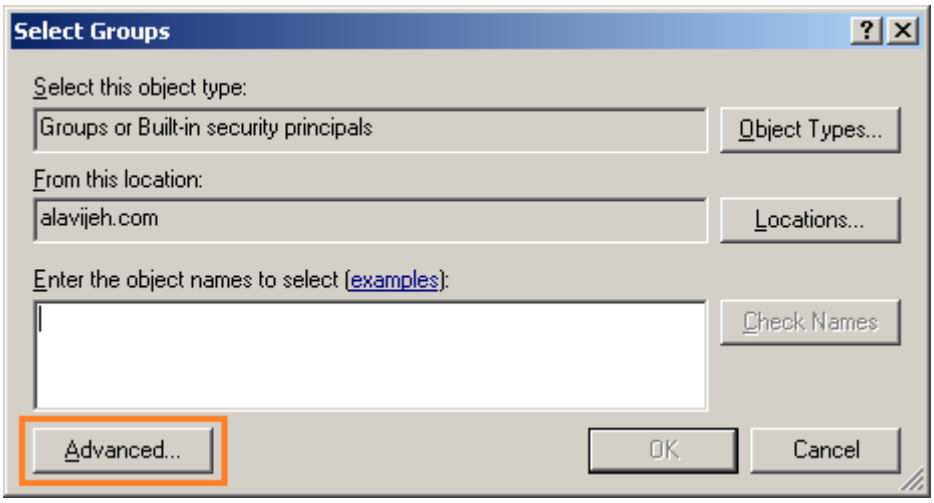


سپس روی کاربر مورد نظر راست کلیک کرده و گزینه Properties را انتخاب نمایید.

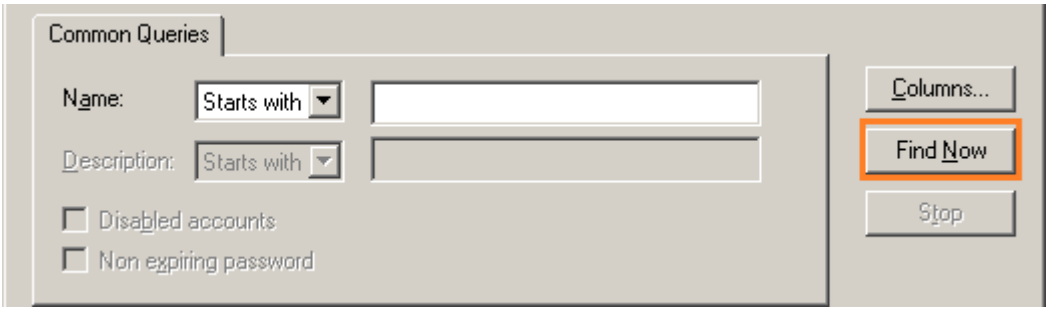
سپس در صفحه باز شده، وارد سربرگ Member of شوید. برای عضویت این کاربر در گروهی خاص، روی دکمه Add کلیک کنید.



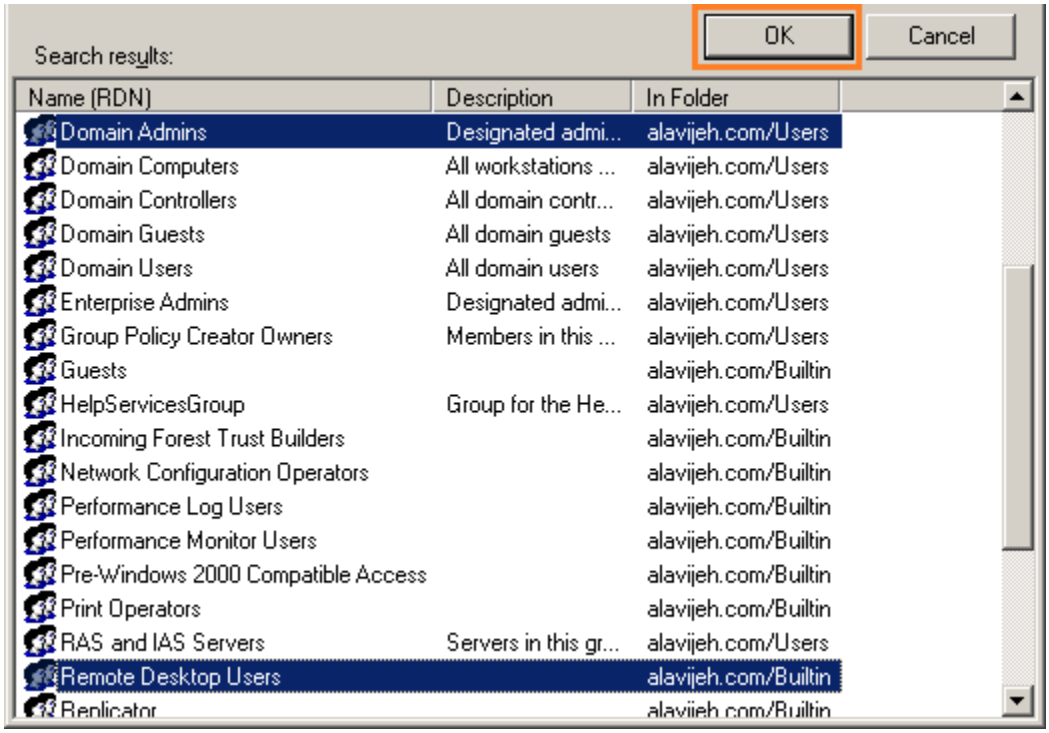
در صفحه باز شده، دو راه پیش رو دارید. راه اول وارد کردن متن Remote Desktop Users;Domain Admins و سپس کلیک روی دکمه Check Names است. راه دیگر انتخاب دو گروه فوق به صورت Visual (بصری) است. بدین منظور روی دکمه Advanced کلیک کنید.



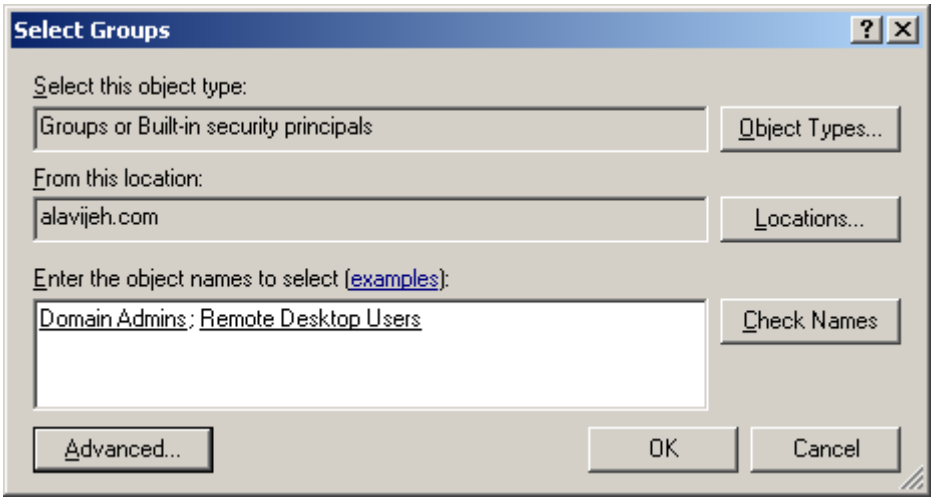
در صفحه باز شده، روی دکمه Find Now کلیک کنید تا لیست گروه های سیستم نمایان شود.



پس از نمایان شدن لیست گروه ها، دو گروه Remote Desktop Users و Domain Admins را انتخاب کرده و روی دکمه OK کلیک کنید.



در صفحه زیر، نام دو گروه انتخاب شده را مشاهده می کنید. روی دکمه OK کلیک کنید.

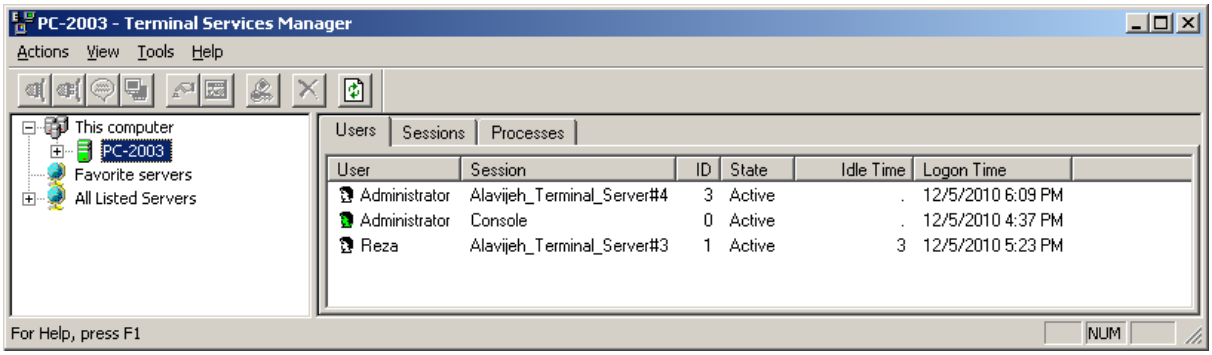


با انجام این امور می توانید، توسط کاربر انتخاب شده در فوق به صورت Remote به سیستم دسترسی یابید. برای این دسترسی از نرم افزار Remote Desktop استفاده نمایید.

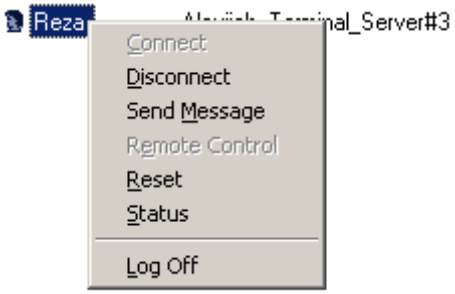
۲۴-۶- Terminal Service Manager

در معرفی Terminal Server گفتیم که یکی از مزایای Terminal Server، قابلیت مدیریت کاربران Login کرده به سیستم می باشد. یعنی در Server می توان کاربرانی را که به صورت Remote به Server وارد شده اند را مدیریت کرد. بدین منظور از ابزار Terminal Service Manager استفاده می کنیم. برای دسترسی به این ابزار، از مسیر Start ➔ Administrative Tools، گزینه Terminal Service Manager را انتخاب نمایید.

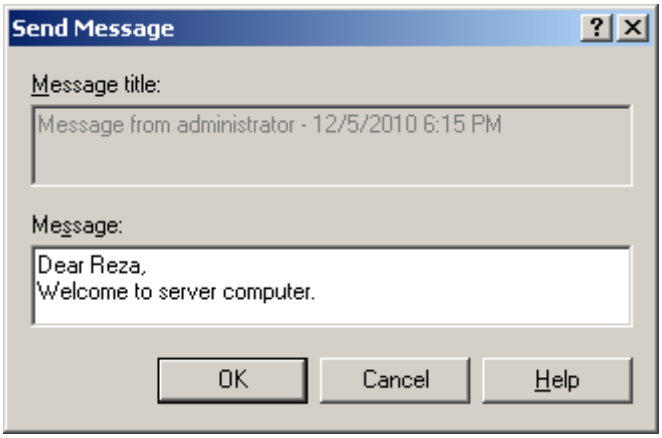
با انتخاب این برنامه، صفحه ای مانند زیر باز می شود. اگر از قسمت سمت چپ و بخش This Computer، نام Server را انتخاب کنید، مانند شکل زیر نام کاربران Login کرده را مشاهده خواهید کرد. در این شکل، ما توسط کاربر Administrator به صورت Local (محلی – ورود به سیستم به صورت مستقیم) و توسط کاربران Administrator و Reza به صورت Remote به سیستم Login کرده ایم. آن هایی که در قسمت Session، کلمه Console قرار گیرد، بیانگر کاربرانی می باشد که به صورت Local به سیستم وارد شده اند؛ اما بقیه بیانگر کاربرانی می باشد که به صورت Remote به سیستم وارد شده اند.



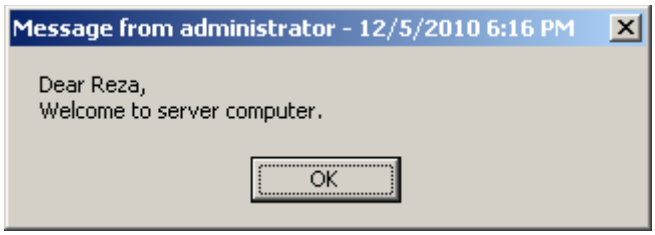
با راست کلیک روی نام کاربر، انواع عملیات قابل انجام را خواهید دید. این عملیات عبارتند از قطع ارتباط، ارسال پیغام به کاربر، Reset کردن ارتباط، مشاهده وضعیت کاربر و اخراج (Log Off) کاربر.



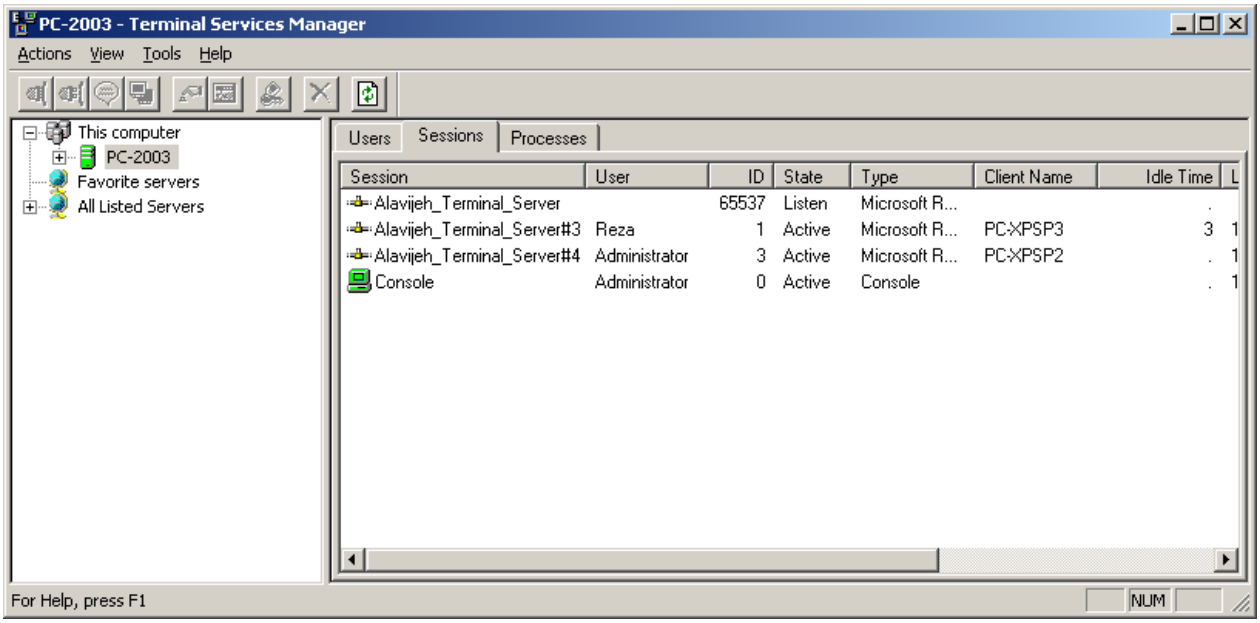
یکی از کاربردهای ارسال پیغام، هشدار دادن به کاربر و توجه دادن کاربر به این موضوع است که ما کارهای کاربر را مشاهده نموده و مراقب او هستیم. پس از راست کلیک کردن روی نام کاربر و انتخاب گزینه Send Message، صفحه زیر نمایان می شود. پس از وارد کردن پیغام، روی دکمه OK کلیک کنید.



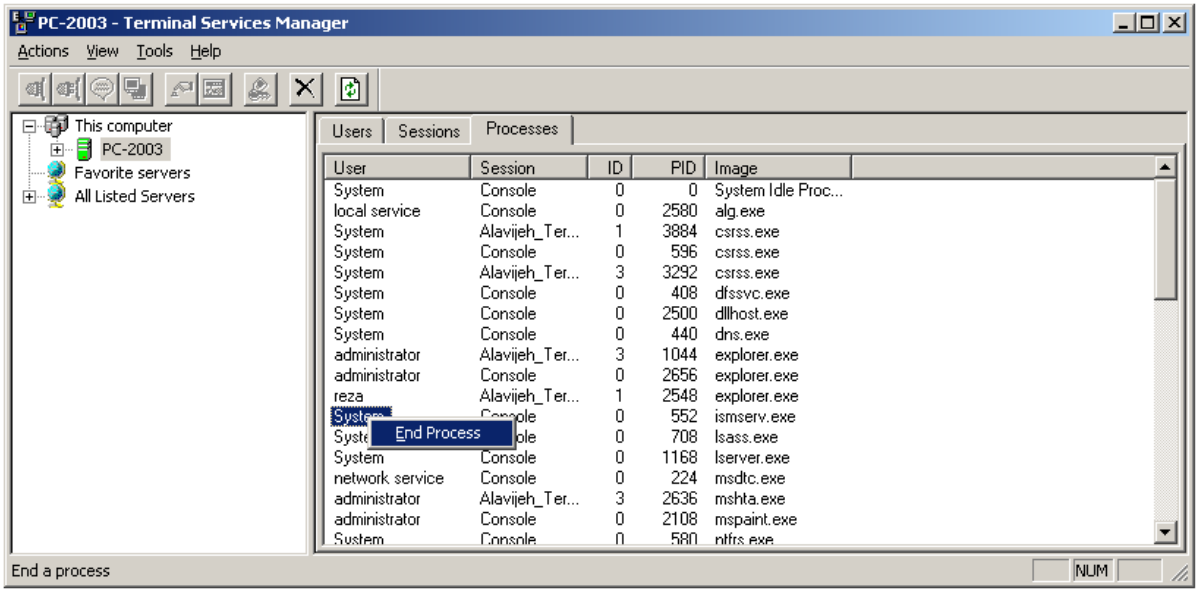
پس از این کار، کاربر راه دور، مانند شکل زیر پیام شما را مشاهده خواهد نمود.



اگر در همین صفحه، وارد سربرگ Session شوید، لیست Sessionهای (جلسه - نشست) ایجاد شده را مشاهده خواهید نمود.



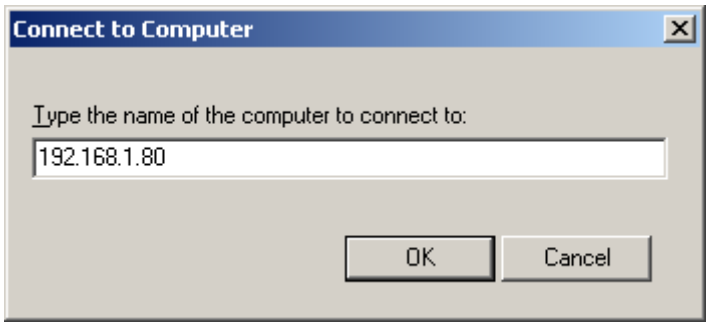
در همین صفحه، اگر وارد سربرگ Processes شوید، لیست تمام پردازش هایی که کاربران راه دور روی سیستم شما اجرا کرده اند را مشاهده خواهید نمود. ستون User بیانگر نام کاربری می باشد که این پردازش را اجرا کرده است. برای بستن یک پردازش، روی آن راست کلیک کرده و گزینه End Process را انتخاب نمایید.



در قسمت سمت چپ، گزینه ای تحت عنوان All Listed Servers وجود دارد. در این قسمت لیست Serverهایی که دارای Terminal Server بوده و به آن متصل شده ایم را مشاهده خواهید نمود.

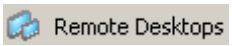
برای اتصال به Serverی دیگر که دارای Terminal Server می باشد، روی All Listed Servers راست کلیک کرده و گزینه Connect to Computer را انتخاب کنید.

در صفحه باز شده، نام یا آدرس IP کامپیوتر Server را وارد کرده و روی OK کلیک کنید. پس از اتصال قابلیت کنترل Server انتخاب شده را خواهید داشت.

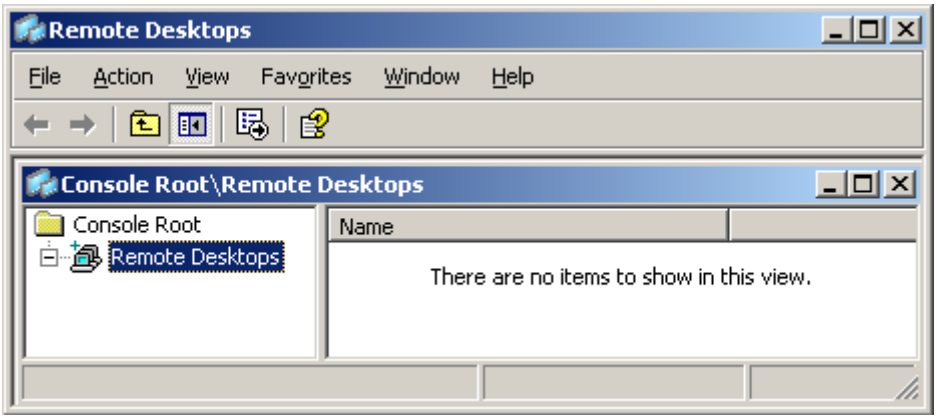


۲۴-۷- استفاده از Remote Desktop Connection در ویندوز سرور ۲۰۰۳

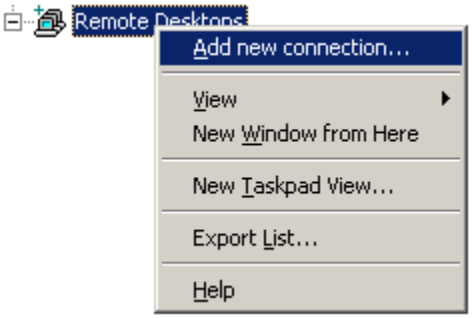
ویندوز سرور نیز مانند ویندوز XP، دارای ابزار Remote Desktop Connection جهت اتصال به سیستم های راه دور می باشد. اما در ویندوز سرور، ابزار قوی تری تحت عنوان Remote Desktops وجود دارد. توسط این ابزار می توان همزمان به چند سیستم راه دور دسترسی داشت و آن ها را کنترل نمود. مزیت دیگر این ابزار، این است که می توان با تنظیم User Name و Password برای یک اتصال برای بار اول، برای اتصال های بعدی دیگر User Name و Password وارد نکرد. برای بازکردن این ابزار، از قسمت Administrative Tools ← Start، برنامه Remote Desktops را اجرا نمایید.



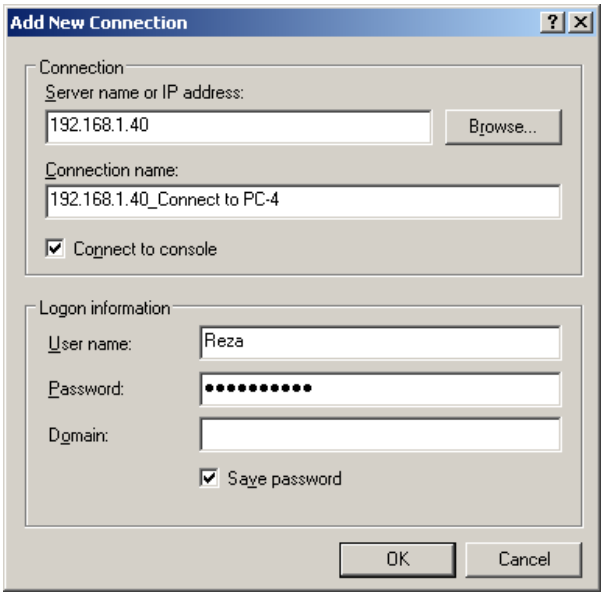
پس از باز شدن برنامه، صفحه ای مانند صفحه زیر را مشاهده خواهید کرد. قسمت سمت چپ، بیانگر اتصالات ساخته شده و قسمت سمت راست بیانگر صفحه کاری شما می باشد.



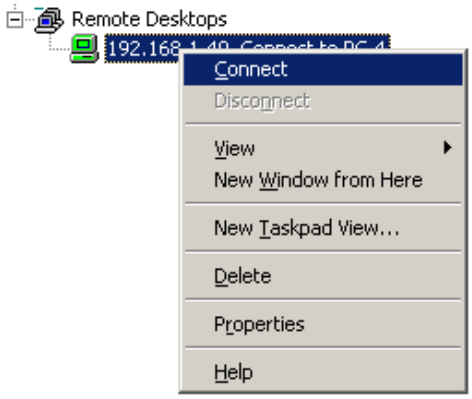
برای ساخت اتصال جدید، روی قسمت Remote Desktops راست کلیک کرده و Add new connection را انتخاب نمایید.



در صفحه باز شده، ابتدا آدرس IP یا نام کامپیوتر مقصد را وارد کنید. سپس یک نام برای Connection خود انتخاب نمایید. در نهایت نیز نام کاربری، رمز عبور و نام دامنه (در صورتی که نام کاربری وارد شده، مربوط به دامنه ای خاص بوده که کامپیوتر مقصد به آن متصل می باشد) را وارد کرده روی OK کلیک کنید. در صورتی که گزینه Save Password را فعال کرده باشید، برای اتصالات بعدی، نیازی به وارد کردن رمز عبور نخواهید داشت.



برای اتصال به کامپیوتر راه دور، روی Connection ساخته شده راست کلیک کرده و گزینه Connect را انتخاب نمایید.



پس از اتصال، صفحه کامپیوتر راه دور را در سمت راست مشاهده خواهید کرد.

البته توجه نمایید که اگر سیستم عامل کامپیوتر راه دور شما، ویندوز سرور نباشد، کاربر جاری آن از سیستم خارج (Log out) خواهد شد.

هنگام بستن برنامه Remote Desktops، سیستم از شما سوالی مبنی بر ذخیره اطلاعات اتصالات ساخته شده می پرسد. به سوال پرسیده شده، جواب مثبت بدهید تا اطلاعات شما ذخیره شود.

Remote Assistance -۸-۲۴

قابلیت Remote Assistance، به معنای دستیار از راه دور، وسیله ای است که از آن برای کنترل و ایجاد تغییرات در یک رایانه دیگر به کار می رود. به طور کلی این قابلیت برای استفاده توسط اشخاصی است که قرار است رایانه هایشان را از طریق اینترنت به یکدیگر متصل کنند تا یکی به عنوان مددکار و دیگری به عنوان درخواست کننده عمل کنند. اما مددکار کیست؟ شخصی که با رایانه اش به عنوان یک متخصص یا تعمیرکار نرم افزار کامپیوتر، توسط درخواست کننده در قالب یک فرم به نام

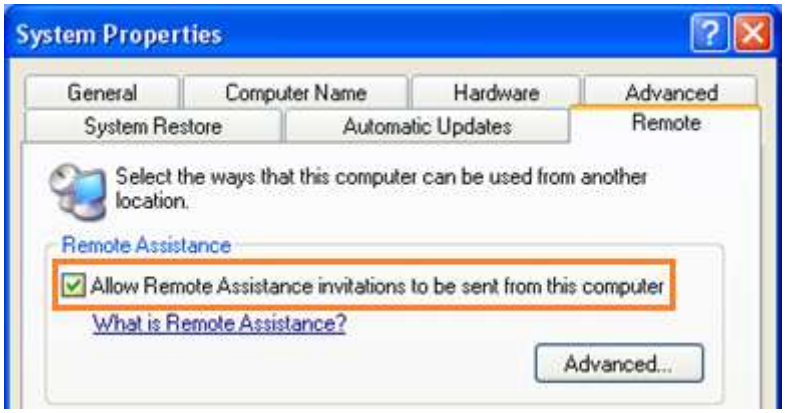
Invitation (دعوتنامه) فراخوانده می شود. متاسفانه این قابلیت فقط در ویندوز XP وجود دارد و لازمه استفاده از آن، موجود بودن ویندوز XP در هر دو رایانه است. به طور کلی در همه شرایط و در تمامی برنامه های Remoting، یک برنامه Client و یک برنامه Server وجود دارد. در این نوع برنامه ها کاربر درخواست کننده که گاهی Assist نامیده می شود با ایجاد و ارسال یک Invitation از طریق یک Email (که در واقع یک دعوتنامه به صورت فایل می باشد) برای رایانه مددکار ارسال می کند. کاربر مددکار با باز کردن Email و اجرای فایل Invitation (دعوتنامه) به صورت خودکار به سیستم درخواست کننده متصل خواهد شد.

۲۴-۸-۱- طریقه فعال سازی Remote Assistance

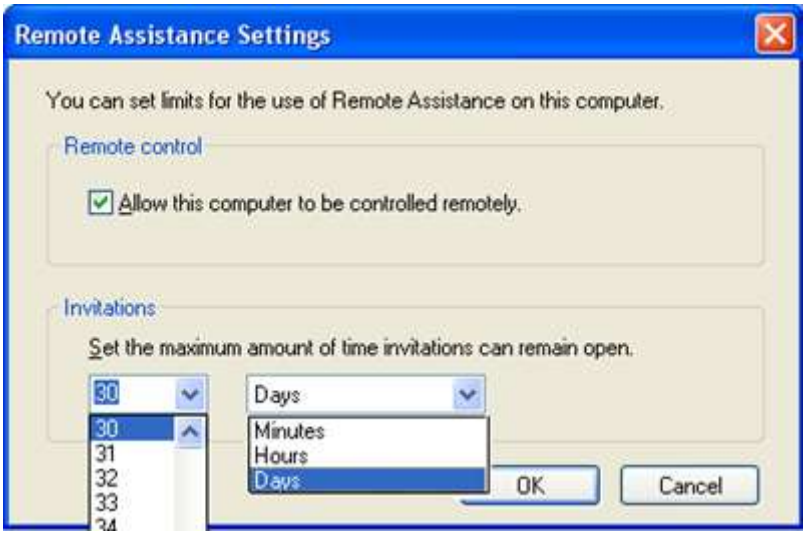
کاربری که Invitation تولید می کند قبل از استفاده از ابزار Remote Assistance و ایجاد فایل دعوتنامه می بایست در تنظیمات ویندوز این قابلیت را فعال نماید تا کاربر مددکار بدون هیچ مشکلی به آن سیستم وصل شده و به رفع عیوب بپردازد. برای دسترسی به تنظیمات فعال سازی Remote Assistance مسیرهای متفاوتی وجود دارد که در ابتدا نیاز به پنجره System Properties داریم.

۱. مسیرهای متفاوت آن شامل Start ➔ Control Panel ➔ System یا از طریق کلیک راست کردن روی My Computer و انتخاب Properties می باشد.

۲. در پنجره System Properties برگه Remote را انتخاب می کنیم. همانطور که مشاهده می کنید ابتدای برگه از ما درخواست شده که نوع ارتباط از موقعیت های دیگر را انتخاب کنیم. از فرم اول (Remote Assistance)، چک باکس allow Remote Assistance Invitation to be sent from this computer را تیک دار می کنیم. در اینصورت از این پس اجازه استفاده از این قابلیت داده می شود که شامل ارسال دعوتنامه می شود:



۳. روی دکمه Advanced در همین پنجره کلیک کرده و در پنجره Remote Assistance Setting گزینه Allow this computer to be controlled Remotely. را تیک دار کنید. با این عمل به کامپیوتر مددکار اجازه می دهید که جهت رفع عیوب به سیستم شما متصل شود. هر دعوتنامه ای که برای رایانه مددکار می فرستید دارای اعتبار و میزان مدت زمان مشخص شده می باشد که این زمان همانطور که در شکل ملاحظه می کنید بر حسب تعداد ساعت، روز و ماه از فرم Invitation در همین پنجره قابل تنظیم می باشد:



۲۴-۸-۲- نکات مهم حین استفاده از Remote Assistance

۱. هنگام اتصال Firewall سیستم باید غیر فعال باشد تا هنگام اتصال از طریق پورت های سیستم عامل مشکلی در اتصال به وجود نیاید.
۲. کاربر مبتدی هنگامی که فرم Invitation را پر می کند می بایست به اینترنت متصل باشد.
۳. بعد از اتمام فرم و تولید فایل مربوطه مشخصات IP شما در این فایل ثبت می شود تا بعد از اجرای فایل توسط مددکار، وی امکان اتصال به رایانه درخواست کننده را داشته باشد.
۴. پس از تولید فایل دعوتنامه تا هنگام اتصال به مددکار، درخواست کننده نباید از اینترنت Disconnect شود؛ زیرا در صورت استفاده نکردن از IP ثابت، با هر بار اتصال به اینترنت و ISP مربوطه، سرویس DHCP (که وظیفه توزیع IP را دارد) یک IP جدید تولید کرده که با مشخصات فایل ارسال شده برای مددکار متفاوت است و مددکار نمی تواند رایانه شما را از طریق فایلتان پیدا کند.
۵. در صورت استفاده از IP ثابت مانعی برای قطع اتصال اینترنت و اتصال مجدد وجود ندارد. بهترین کار این است که درخواست کننده و مددکار از طریق Online شدن و با نرم افزار های Messenger بتوانند از متصل بودن یکدیگر به اینترنت مطلع شوند.

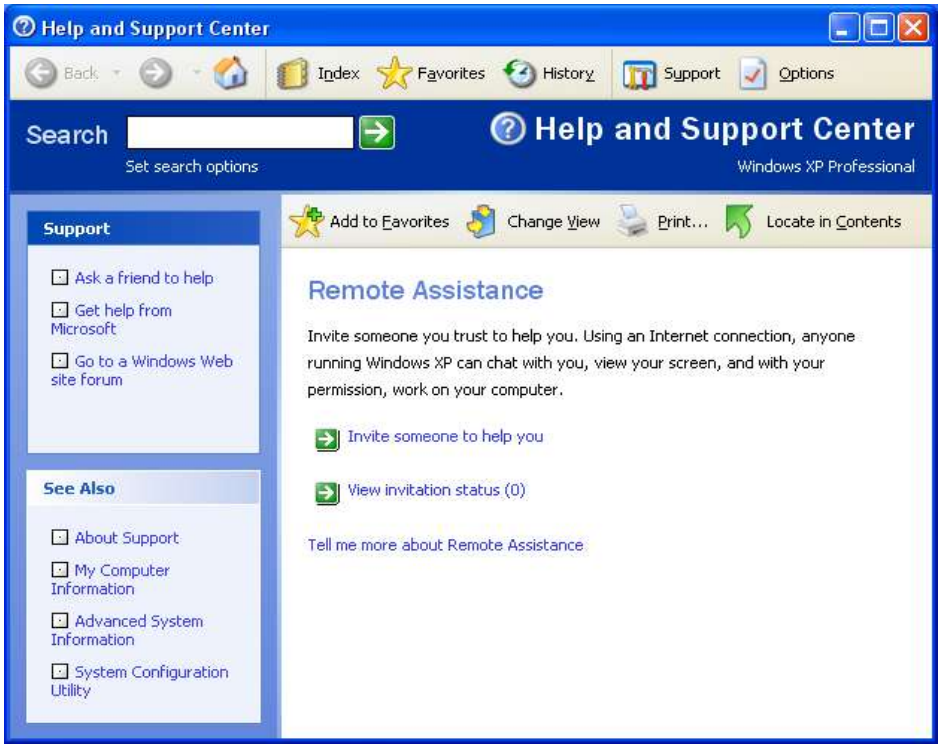
۲۴-۸-۳- روش ایجاد یک Invitation (دعوتنامه) توسط درخواست کننده

برای ایجاد یک دعوتنامه توسط درخواست کننده ابتدا باید از اتصال به اینترنت اطمینان حاصل کرد. سپس از دو روش می توان به Remote Assistance دسترسی داشت:

روش اول: Start ➔ All Programs ➔ Remote Assistance

روش دوم: فشردن دکمه F1 و وارد به پنجره Help اصلی ویندوز و در قسمت Ask for Assistance انتخاب گزینه اول:
Help Invite a friend to connect to your computer with Remote Assistance

پس از طی هر کدام از مسیر های بالا پنجره Help مربوط به Remote Assistance ظاهر می شود:



در این صفحه اگر قبلاً دعوتنامه ای ایجاد نکرده باشید، روبروی گزینه View Invitation status مقدار صفر (۰) نمایش داده خواهد شد. برای ایجاد دعوتنامه در همین پنجره روی گزینه Invite someone to help you کلیک کنید.

۲۴-۸-۴- انواع روش ساخت دعوتنامه

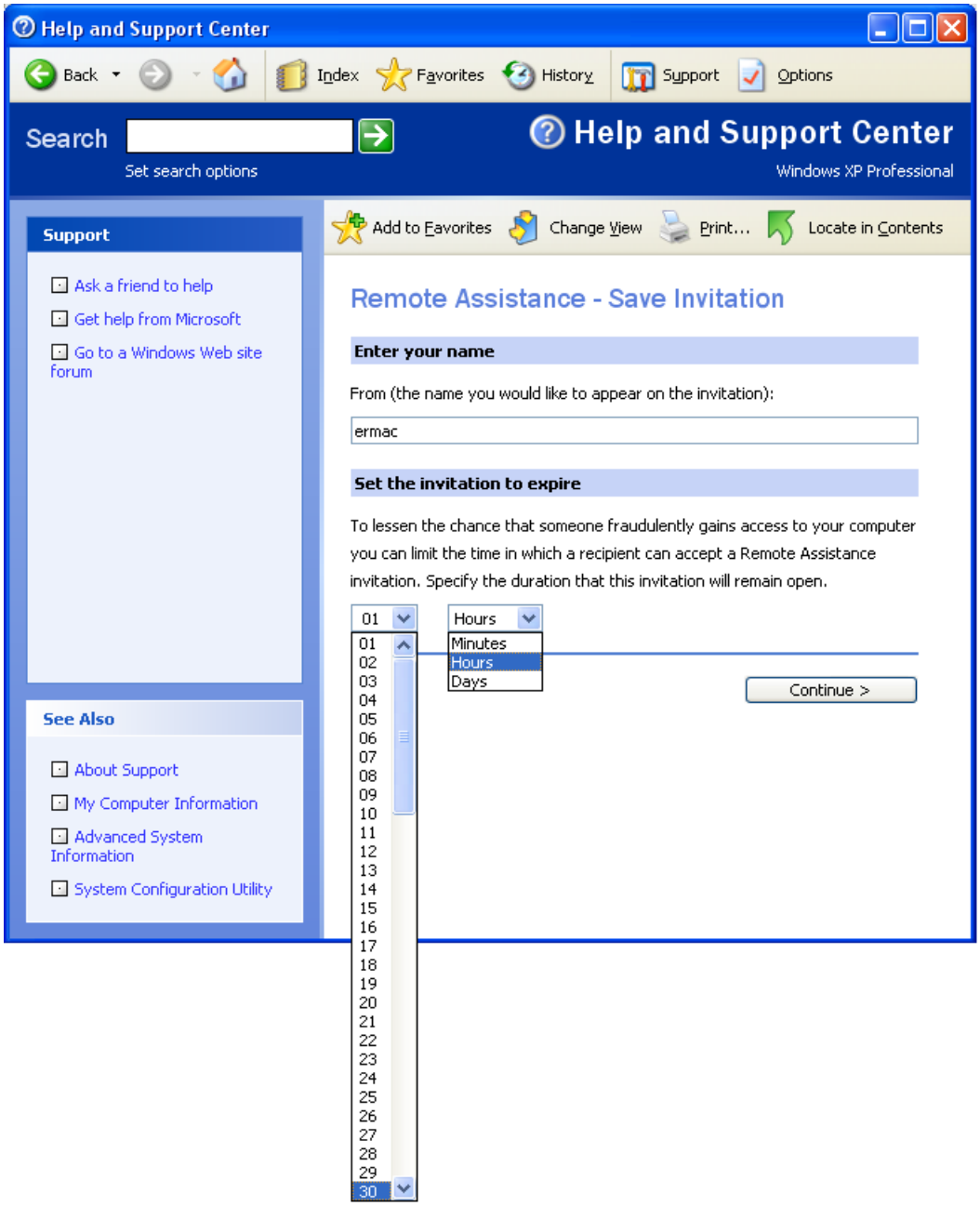
ساخت دعوتنامه در محیط Help با سه روش زیر امکانپذیر است:

۱. روش اول استفاده از Windows Messenger می باشد. کاربر درخواست کننده باید یک حساب در سایت Hotmail یا MSN داشته باشد و بعد از Sing In شدن و پر کردن فرم مربوط به دعوتنامه قابلیت ارسال آن را به شخص مددکار خواهد داشت.

۲. در روش دوم درخواست کننده از نرم افزار Outlook Express برای ارسال فرم دعوتنامه استفاده می کند که قبل از استفاده از آن می بایست تنظیمات کلی مبنی بر سرور SMTP مربوطه اعمال شود.

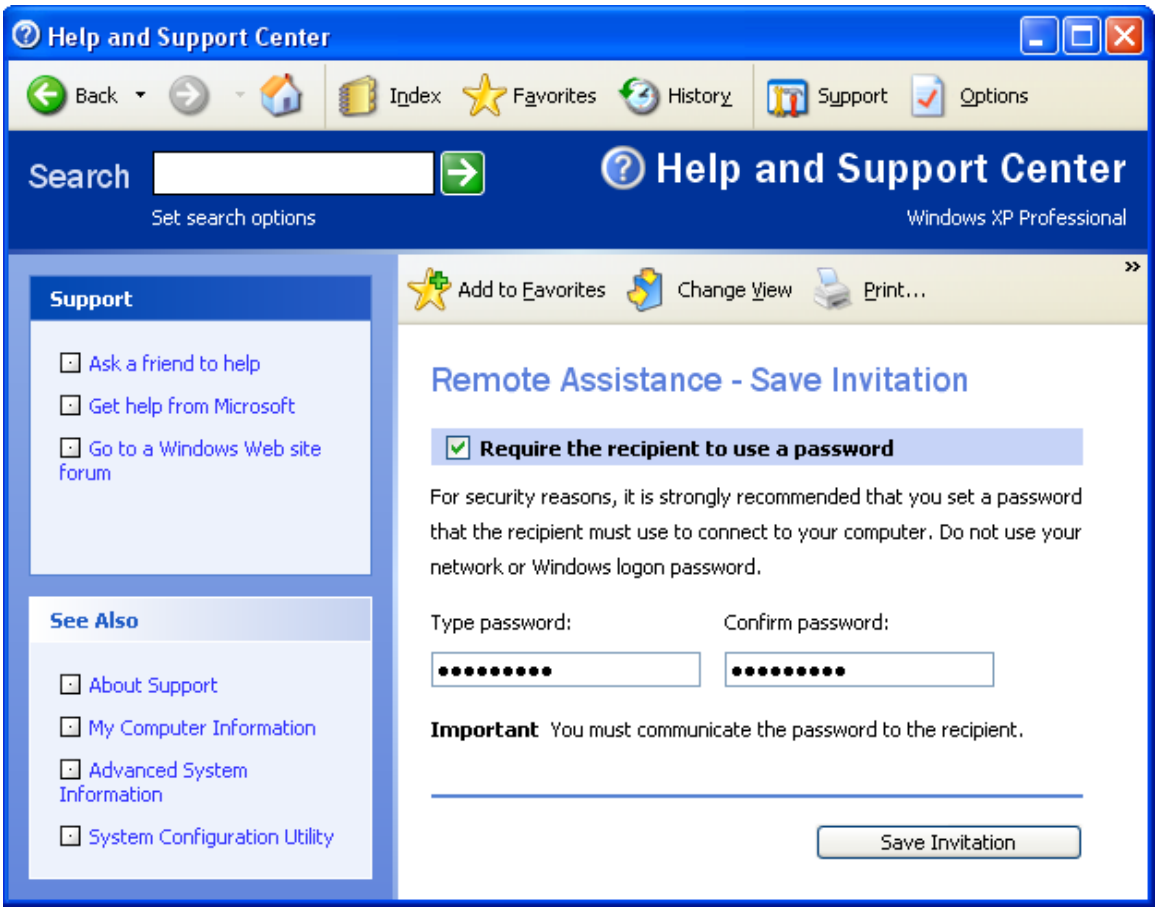
۳. روش سوم و بهترین روش استفاده از گزینه Save Invitation As A File (Advanced) می باشد که با استفاده از این روش، سیستم فایلی را با عنوان RAInvitation.msrcinccident و به حجم بسیار ناچیز (حدود ۱Kbyte) تولید می کند. کاربر درخواست کننده به راحتی به سیستم ایمیل خود مانند Yahoomail، Gmail و... وصل شده و این فایل را به یک نامه Attach کرده (روش اتصال یک فایل به متن یک ایمیل) و به آدرس ایمیل مددکار ارسال می کند. در دو روش اول و دوم، Windows Messenger و Outlook Express بطور خودکار یک ایمیل تولید می کنند و این فایل به آن Attach شده و ارسال می شود اما روش سوم به صورت دستی و Attach کردن آن به هر ایمیل به هر آدرسی امکانپذیر است.

پس از انتخاب روش سوم (روش پیشنهادی برای ادامه کار) و ایجاد فایل مذکور پنجره زیر ظاهر خواهد شد:

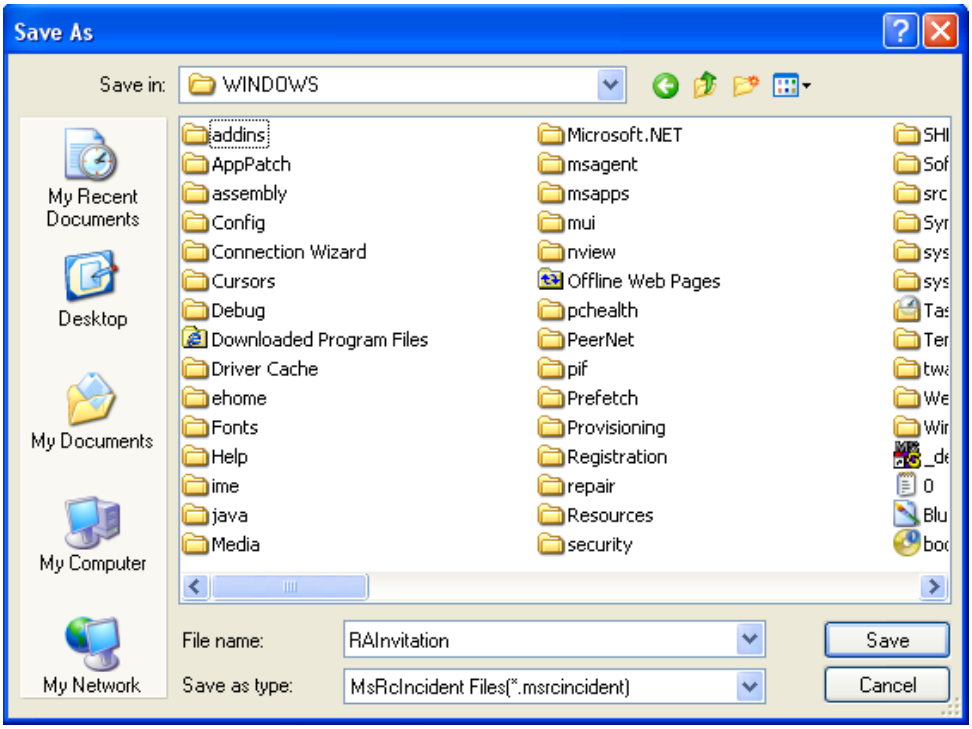


در این پنجره شما باید نام و مدت زمان اعتبار دعوتنامه خود را مشخص کنید. مدت زمان اعتبار دعوتنامه به صورت تعداد دقیقه، ساعت و روز تنظیم می شود. در واقع پس از به پایان رسیدن این مدت زمان ارتباط به طور خودکار قطع شده و اعتبار دعوتنامه از بین خواهد رفت. در این حالت مددکار برای برقراری ارتباط مجدد نیاز به یک دعوتنامه جدید از طرف درخواست کننده دارد.

با تکمیل پنجره بالا و انتخاب دکمه Continue، پنجره زیر ظاهر می شود:



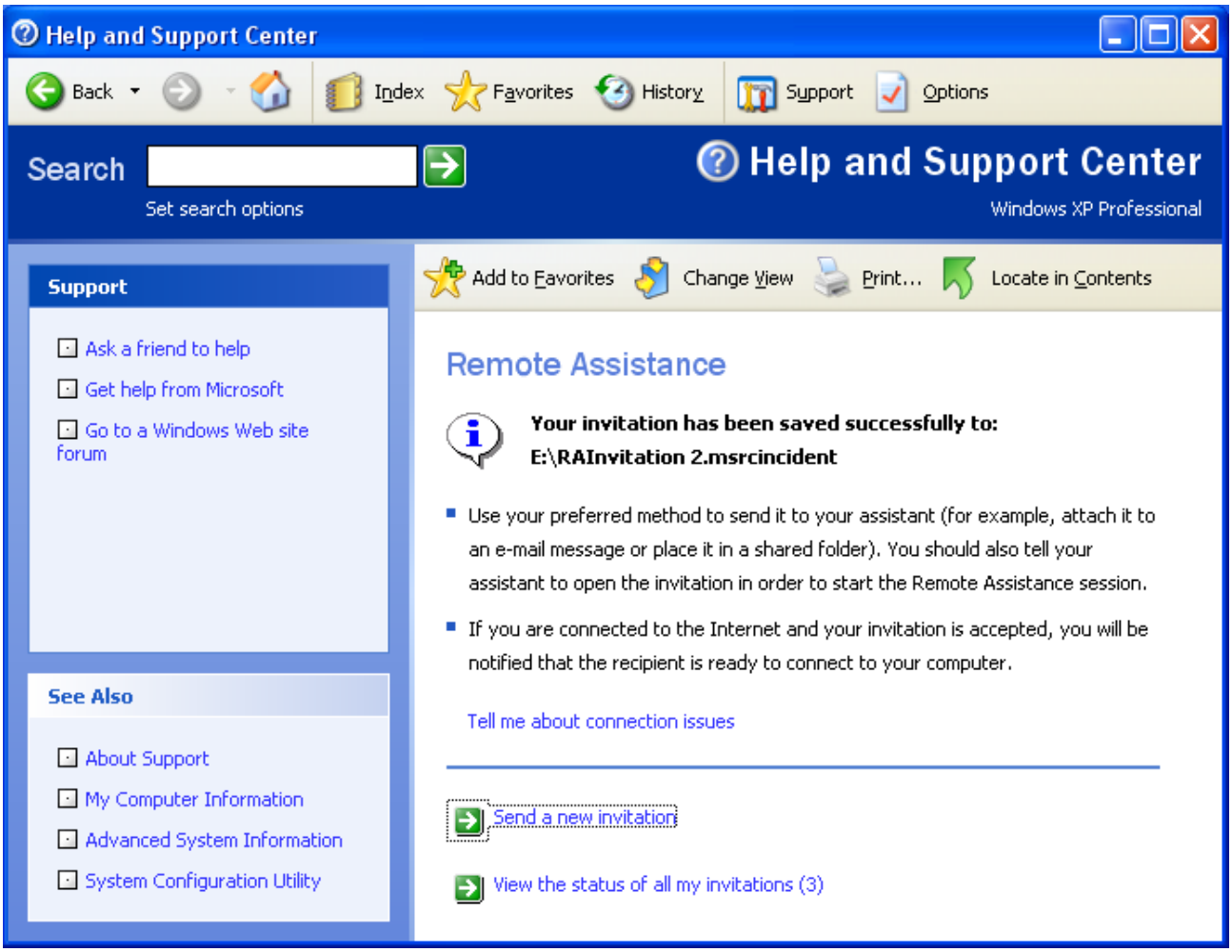
در این پنجره کاربر درخواست کننده با انتخاب یک Password برای دسترسی و اتصال کاربر مددکار به فرم انتخاب می کند که البته این رمز باید از قبل در اختیار مددکار قرار گذاشته شده باشد. پس از انتخاب رمز و فشردن دکمه Save Invitation پنجره محاوره ای Save As ایجاد شده که از شما درخواست انتخاب یک مسیر مناسب برای ذخیره فعلی فایل RAInvitation را دارد:



آیکون فایل ساخته شده و ذخیره شده به شکل زیر می باشد:

RAInvitation

پس از انتخاب مسیر مورد نظر برای ذخیره فایل دعوتنامه پنجره زیر ظاهر می شود که عدد مقابل گزینه view the status of all my Invitation (به عنوان مثال در اینجا ۳) نشان دهنده تعداد فایل های درخواست تولید شده است:

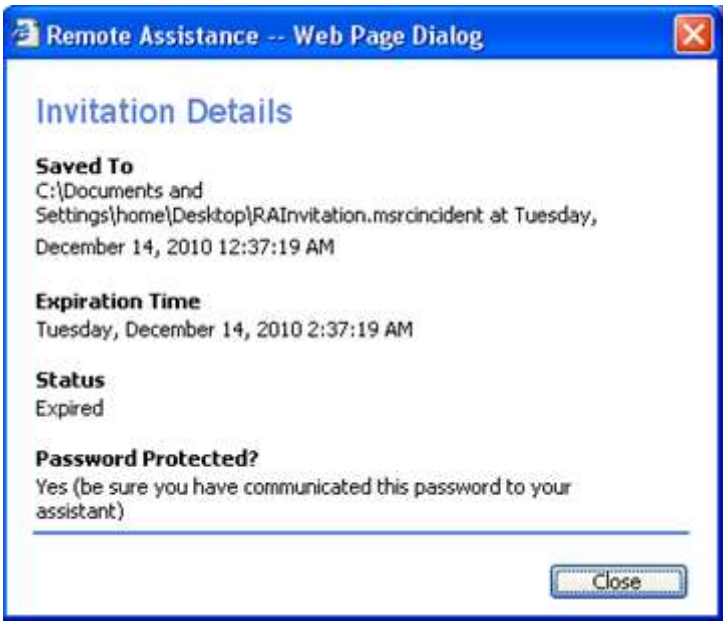


با انتخاب همین گزینه می توان تعداد و جزییات فایل های ساخته شده را در پنجره زیر مشاهده کرد:

در این پنجره تعداد سه فایل ساخته شده با روش سوم مشاهده می شود که با انتخاب هر کدام از فایل ها می توان آن ها را:

- با دکمه Delete آن را حذف نمود.
- با دکمه Resend... تعویض نام و رمز و مدت اعتبار برای ارسال مجدد فایل Expire شده، (Expired فایلی است که اعتبار آن تمام شده است)
- با دکمه Expire، آن را غیر معتبر نمود.

- و با استفاده از دکمه Details وضعیت فایل را در پنجره ای دیگر مشاهده کرد که شامل محل ذخیره سازی فایل، تاریخ به پایان رسیدن اعتبار، وضعیت در حال حاضر فایل و در نهایت یک تائیدیه Password که در یک پنجره درج می شود. پنجره زیر مربوط به Details فایل سوم می باشد:



پس از مشاهده فایل دعوتنامه، آماده ارسال با هر روشی (ایمیل- فلش و...) به مددکار می باشد.

۲۴-۸-۵- روش استفاده از فایل Invitation توسط مددکار

حال وظیفه مددکار پس دریافت دعوتنامه چیست؟ کاربر مددکار فایل RAInvitation را دریافت می کند. در ابتدا باید از Online بودن درخواست کننده مطلع شود که از طریق Windows Messenger می تواند این هماهنگی را با درخواست کننده ایجاد کند. پنجره زیر که همان Invitation (دعوتنامه) می باشد، شامل محل ورود Password درخواست کننده است که مددکار با فشردن yes متصل می شود.

۲۴-۹- تفاوت های Remote Desktop و Remote Assistance

سوال مطرح شده درباره این دو قابلیت شبیه به هم ویندوز این است که چرا مایکروسافت هر دو قابلیت را در یک نرم افزار قدرتمند ارایه نکرده و تفاوتهای آنها در چیست؟

اولین تفاوت در روش استفاده و ارتباط کاربر Client و کاربر Server می باشد. نرم افزار Remote Desktop یک ابزار ویرایش شده از نرم افزار Terminal Server در ویندوز ۲۰۰۳ می باشد. در این نرم افزار رایانه درخواست کننده که قسمت Server را در اختیار دارد می بایست از ویندوز نسخهXP یا ۲۰۰۳ استفاده کند ولی رایانه مددکار که به عنوان Client عمل می کند می تواند از هر سیستم عاملی استفاده کند. به عنوان مثال اگر مددکار از ویندوز ۹۸ استفاده کند، تنها با قرار دادن سی دی ویندوز

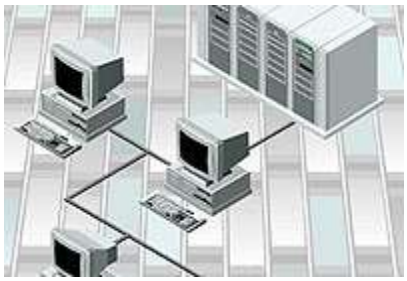
XP در سی دی رام و نصب نرم افـزار Set Up Remote Desktop Connection از گزینـه Perform Additional Tasks مـی تواند از این ابزار جهت اتصال اسـتفاده کنـد. امـا نـرم افـزار Remote Assistance فقـط در ویـنـدوز XP وجـود دارد و رایانـه درخواست کننده و مددکار بالاجبار می بایست از این سیستم عامل استفاده کنند. برنامه Remote Assistance نیازی به ابـزار Client ندارد و خودش به عنوان Server-Client عمل می کند، به این صورت که مددکار از یـک درخواسـت در قالـب XML استفاده می کند که با خاصیت XML نیازی به نصب نرم افزار اضافی مانند Remote Desktop Connection نمی باشد.

نکته دیگر Authentication یا تشخیص هویت کاربر در این سیستم ها می باشد. کاربران برای اسـتفاده از Remote Desktop باید در ویندوز سیستمی که قرار است به آن متصل شوند، یک Account تعریـف شـده داشـته دارنـد. ایـن Account توسـط Administrator (یا همان مدیر سیستم) به صورت دستی و با مجوز های مشخص با یک کد کـاربری و Password ثبـت مـی شود که تشخیص هویت کاربر متصل شونده به سیستم از طریق سیستم تشخیص ویندوز صورت می گیـرد. امـا در Remote Assistance تشخیص هویت به گونه ای دیگر انجام می گیرد، در این اتصال کـاربر مـددکار، نیـازی بـه داشـتن Account در ویندوز ندارد. کاربر درخواست کننده که اقدام به تولید Invitation برای کـاربر مـددکار مـی کنـد در هنگـام پـر کـردن فـرم دعوتنامه یک Password تعیین می کند که این رمز خود به صورت رمز نگاری شده و بـا پسـوند msrcincident ذخیـره مـی شود. این فایل به هر روشی که به مددکار برسد برای اتصال به سیستم درخواست کننده حتما باید از کلمه عبور تعیـین شـده استفاده شود که در غیر اینصورت ارتباطی بر قرار نخواهد شد.

فصل ۲۵

VPN , Dial UP

۲۵-۱- چگونه از راه دور به شبکه خانگی خود متصل شویم؟



همانطور که تاکنون متوجه شده اید، کامپیوتر های موجود در یک شبکه محلی، قابلیت تعامل با یکدیگر را دارند. بدین معنا که می توانند با یکدیگر ارتباط برقرار کرده و کاربران هر سیستم، از منابع دیگر سیستم ها استفاده نمایند. لازمه این کار این است که سیستم ها به صورت فیزیکی یا غیر فیزیکی (Wireless) به یکدیگر متصل شده باشند. اما آیا تاکنون به این فکر افتاده اید که سیستمی که کیلومترها از شما فاصله دارد، با اینکه اتصالی به شبکه شما ندارد، چگونه می تواند به شبکه شما متصل شده، جزئی از Workgroup شما به حساب آمده و از منابع سیستم شما استفاده کند؟ همچنین گاهی اوقات شما از یک PC دور هستید اما واقعاً نیاز دارید که به فایل ها و یا اسناد موجود بر روی آن دسترسی پیدا کنید. احتمالاً پس از انجام یک سفر متوجه شده اید که فایل مهمی را جا گذاشته اید. همچنین ممکن است یکی از اعضای خانواده نیاز به کمک شما برای انجام کاری روی PC منزل داشته باشد که اگر در منزل می بودید، این کار را در زمان ۳۰ ثانیه انجام می دادید.

در اینگونه شرایط، باید به سراغ فناوری دسترسی از راه دور بروید. به عبارت ساده تر، این فناوری شامل استفاده از یک کامپیوتر برای دسترسی به فایلهای ذخیره شده بر روی یک کامپیوتر دیگر و یا حتی کنترل آن می باشد. با ابزارهای مناسب و کمی آگاهی می توانید از یک PC برای مشاهده و تعامل با دسکتاپ ویندوز یک PC دیگر در آن سوی جهان بهره گیری نمائید.

ما در این فصل به بررسی دو تکنیک مشهور دسترسی از راه دور خواهیم پرداخت.

نکته ای که بین هر دو روش اتصال وجود دارد، این است که برای برقراری ارتباط بین دو سیستم، نیاز به اتصال اینترنت دارید. منظور ما در اینجا یک اتصال اینترنت باند پهن است. در صورتیکه هنوز به یک اتصال Dial-up متکی هستید، ارتباط شما برای انجام اینگونه اقدامات بیش از حد کند خواهد بود.

توجه نمایید که برای برقراری ارتباط بین یک کامپیوتر با یک شبکه، حتما یکی از کامپیوتر های شبکه بایستی به اینترنت یا خط تلفن دسترسی داشته باشد. کامپیوتر راه دور، به همین کامپیوتر شبکه متصل خواهد شد.

به انجام این عمل، شبکه خصوصی مجازی می گویند. یک شبکه خصوصی مجازی (VPN,VPDN) بسط و توسعه یک شبکه محلی و خصوصی، به گونه ای است که اتصالات شبکه های اشتراکی یا عمومی مانند اینترنت را در بر می گیرد (یعنی کاربران شبکه های عمومی مانند اینترنت را قادر می سازد تا به شبکه خصوصی و محلی شما متصل شوند). یک شبکه خصوصی

مجازی شما را قادر می کند اطلاعات را بین دو کامپیوتر در طول یک شبکه اشتراکی یا عمومی بفرستید، در حالتی که با خصوصیات یک اتصال خصوصی نقطه به نقطه یا به عبارتی نظیر به نظیر برابری بکند.

شبکه خصوصی مجازی (Virtual Private Network) و نیز شبکه خصوصی شماره گیری مجازی (Virtual Private Dialup Network) (در مورد این دو گزینه، بعدا بیشتر توضیح می دهیم) در اذهان، تصور یک مطلب پیچیده برای استفاده و پیاده کنندگان آن به وجود آورده است. اما این پیچیدگی، در مطالب بنیادین و مفهومی آن است نه در پیاده سازی.

این نکته را باید بدانید که پیاده سازی دارای روش خاصی نبوده و هر سخت افزار و نرم افزاری روش پیاده سازی خود را دارا است و نمی توان روش استانداردی را برای کلیه موارد بیان نمود. اما اصول کار همگی به یک روش است.

۲۵-۲- مختصری درباره تئوری

مفهوم اصلی، چیزی جز برقراری یک کانال (Tunnel) ارتباطی خصوصی برای دسترسی کاربران راه دور به منابع شبکه نیست. در این کانال که بین دو نقطه برقرار می شود، ممکن است که از مسیرهای مختلفی عبور کند؛ اما کسی قادر به وارد شدن به این شبکه خصوصی شما نخواهد بود (مگر در صورت تایید اعتبار شدن کاربر). گرچه می توان از هر روشی برای اتصال استفاده نمود اما استفاده آن در خطوط Leased (خطوطی شخصی که توسط یک فرد اجاره شده باشد) کار غیر ضروری است. در ادامه به دلیل آن پی خواهید برد (منظور از Leased، مثلاً کابل کشی مستقیم بین دو کامپیوتر است).

در یک ارتباط، شبکه یا شبکه ها می توانند به کمک اینترنت به هم متصل شوند و از این طریق کاربران از راه دور، به راحتی به شبکه دسترسی پیدا کنند. اگر این روش (اتصال توسط اینترنت) را با روش خطوط اختصاصی فیزیکی (Leased) مقایسه کنیم، می بینید که ارائه یک ارتباط خصوصی از روی اینترنت به مراتب از هر روش دیگری ارزان تر تمام می شود.

از اصول دیگری که در یک شبکه در نظر گرفته شده بحث امنیت انتقال اطلاعات در این کانال مجازی می باشد. یک ارتباط می تواند بین یک ایستگاه کاری و یک شبکه محلی و یا بین دو شبکه محلی صورت گیرد. در بین هر دو نقطه یک تونل ارتباطی برقرار می گردد و اطلاعات انتقال یافته در این کانال به صورت کد شده حرکت می کنند، بنابراین حتی در صورت دسترسی مزاحمان و هکرها به این شبکه خصوصی نمی توانند به اطلاعات رد و بدل شده در آن دسترسی پیدا کنند.

۲۵-۳- راه های اتصال یک کاربر به یک شبکه راه دور

دو روش برای اتصال یک کاربر به یک شبکه راه دور وجود دارد

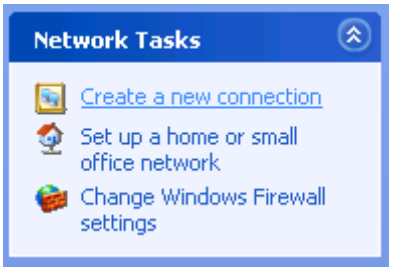
۱. استفاده از خطوط تلفن (VPDN): در این روش، کامپیوتر مبدا، کامپیوتر مقصد را به کمک خط تلفن شماره گیری می کند. در صورتی که کامپیوتر مقصد، کامپیوتر مبدا را بپذیرد، کامپیوتر مبدا جزئی از شبکه کامپیوتر مقصد به شمار خواهد آمد. عیب این روش، هزینه بالای تلفن برای اتصالات غیر شهری است. مزیت این روش این است که نیازی به دانستن آدرس IP کامپیوتر مقصد نداریم.

۲. اتصال از طریق اینترنت (VPN): در این روش، کامپیوتر مبدا ابتدا به اینترنت متصل شده (مثلاً توسط ADSL)، سپس با آدرس IP کامپیوتر مقصد ارتباط برقرار می کند. در صورتی که کامپیوتر مقصد، کامپیوتر مبدا را بپذیرد، کامپیوتر مبدا جزئی از شبکه کامپیوتر مقصد به شمار خواهد آمد. مزیت این روش نسبت به روش قبل، این است که فاصله کامپیوتر ها، هیچ تاثیری بر هزینه نخواهد داشت. اما عیب آن این است که کامپیوتر مقصد باید دارای یک آدرس IP به صورت Valid باشد.

در ادامه به آموزش های عملی انجام این کار می پردازیم.

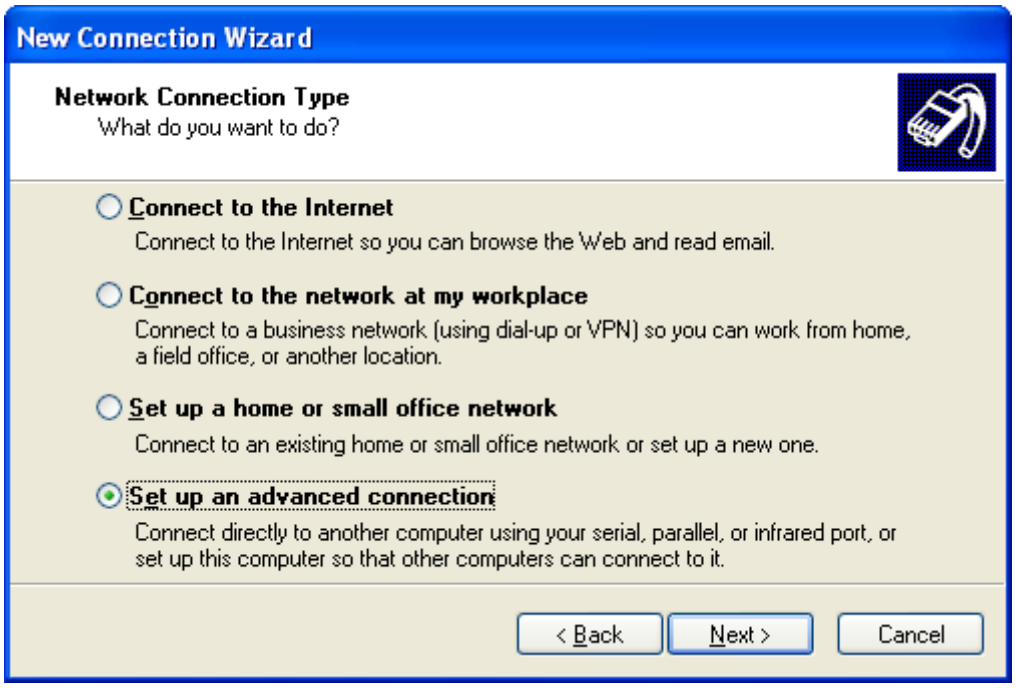
۲۵-۴- آماده سازی ویندوز XP جهت دریافت و پذیرش درخواستها

برای این آماده سازی، ابتدا وارد Control Panel ➔ Network Connection شده و سپس گزینه Create a new connection را انتخاب نمایید.



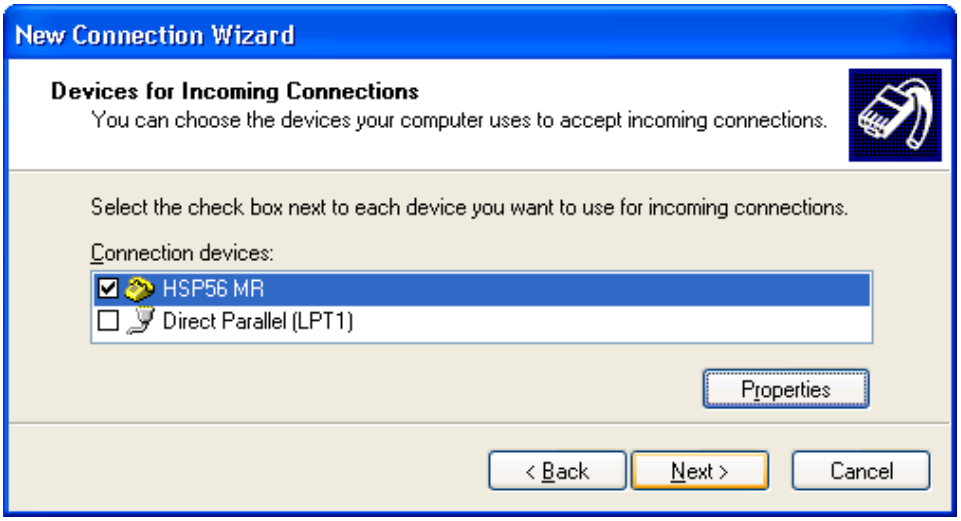
ابتدا صفحه خوش آمد گویی باز می شود. در این صفحه ، روی Next کلیک نمایید.

سپس در صفحه باز شده، گزینه Set up an advanced connection را انتخاب نمایید. این گزینه برای ساخت Connection به منظور ارتباط مستقیم بین کامپیوتر ها است.



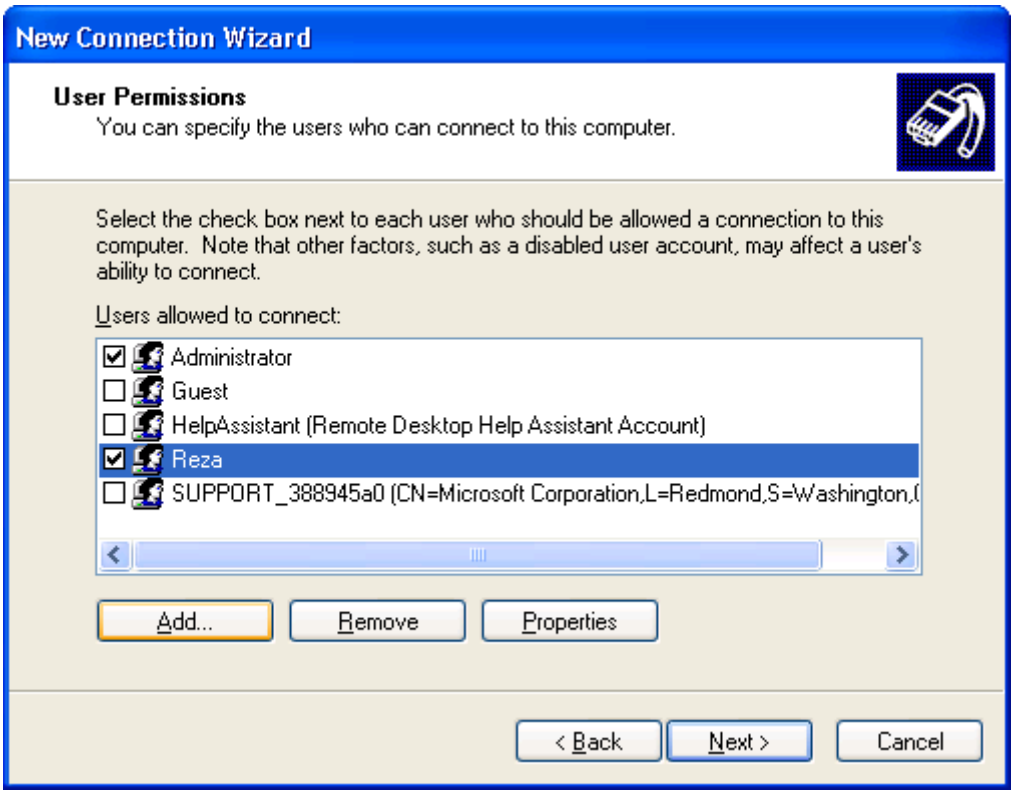
در صفحه بعد، گزینه Accept incoming connections را انتخاب نمایید. این بدان معناست که سیستم درخواست های اتصال را بپذیرد.

در صفحه بعد، وسیله ارتباطی خود را انتخاب نمایید. در این شکل، مودم Dial Up را انتخاب کرده ایم.

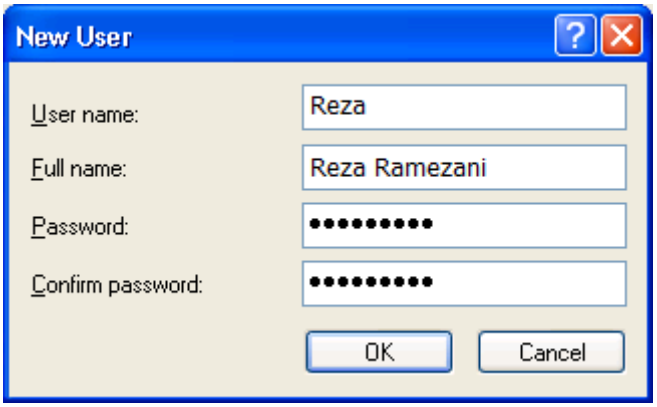


با این کار سیستم شما توسط شماره گیری (VPDN) قابل دسترس خواهد بود. اگر می خواهید که سیستم شما توسط VPN نیز قابل دسترسی باشد، گزینه Allow virtual private connections را انتخاب نمایید.

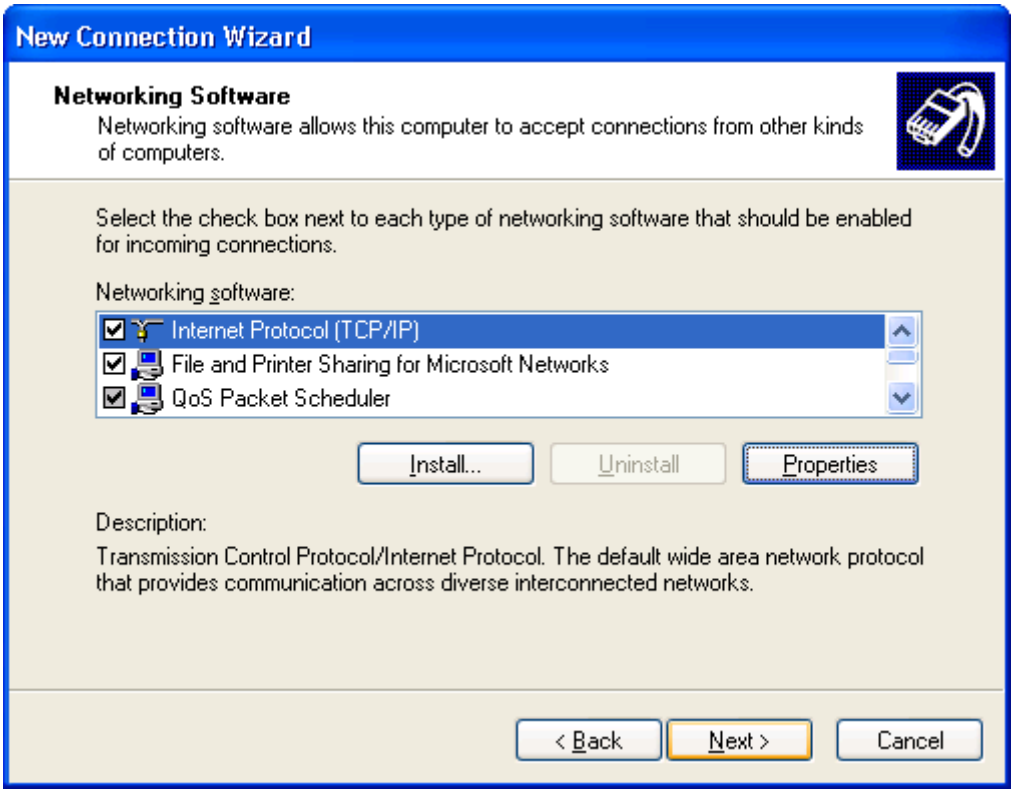
در صفحه بعد، کاربر یا کاربرانی که مجاز به ورود راه دور و استفاده از منابع هستند را انتخاب کنید. در این صورت، هنگام اتصال، بایستی یکی از این نام های کاربری و رمز عبور وی را وارد نمایید.



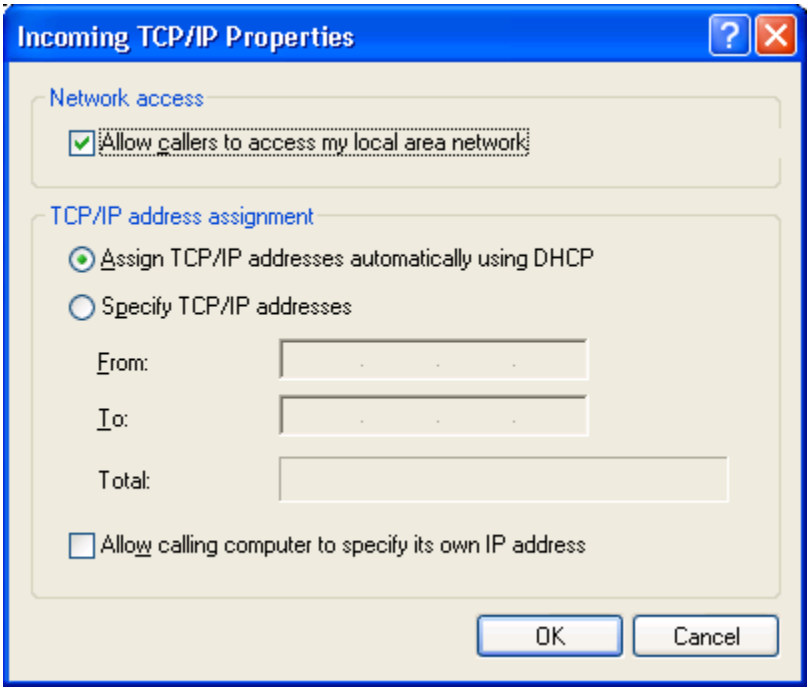
در صفحه قبل، اگر می خواهید، کاربر جدیدی را وارد نمایید، روی دکمه Add کلیک کنید. در صفحه باز شده، اطلاعات کاربر را وارد نمایید. در نهایت OK کرده و Next را بزنید.



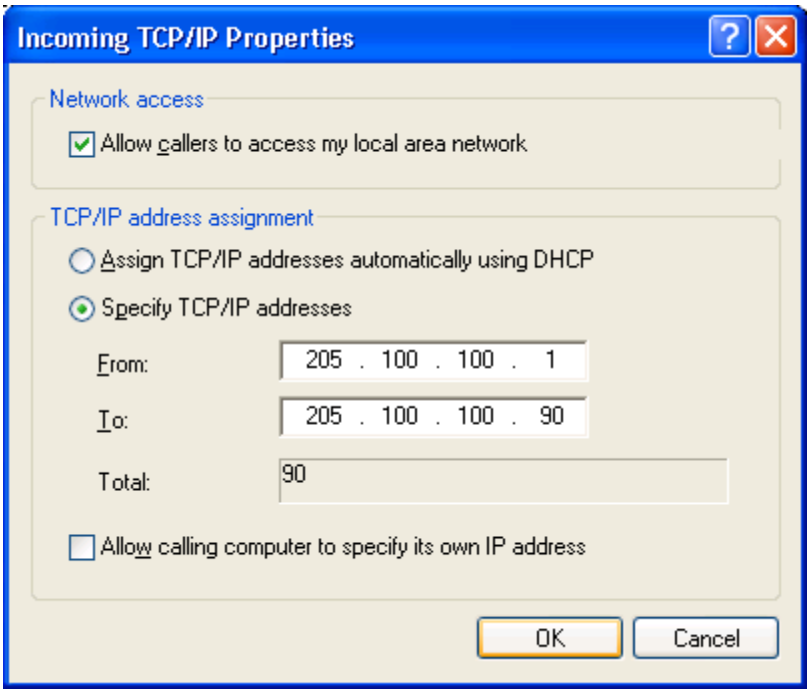
در صفحه بعد می توانید تنظیمات پروتکل خود را انتخاب نمایید. معروف ترین تنظیمات، تنظیم آدرس IP است. بدین معنی که شما بایستی به کاربری که به سیستم شما متصل می شود، یک آدرس IP اختصاص دهید. این آدرس IP باید در محدوده آدرس IP شبکه شما باشد، تا کاربر راه دور بتواند به شبکه شما متصل شود. برای تنظیم آدرس IP، گزینه Internet Protocol را انتخاب کرده و روی Properties کلیک کنید.



در صفحه باز شده، دو ره برای تخصص آدرس IP به کامپیوتر راه دور دارید. راه اول، تخصیص آدرس IP به صورت خودکار و توسط پروتکل DHCP است. با این کار، سیستم از محدوده آدرس IP شما، یک آدرس را انتخاب کرده و به Client تخصیص می دهد. بدین منظور گزینه Assign TCP/IP addresses automatically using DHCP را انتخاب کنید.

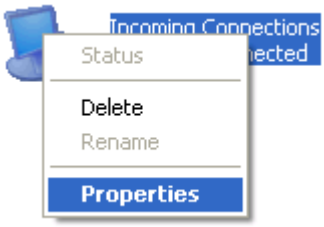


اما اگر قصد دارید که محدوده آدرس IP را خودتان تعیین کنید، بدین منظور گزینه Specify TCP/IP addresses را انتخاب کنید. سپس در قسمت From، آدرس شروع محدوده و در قسمت To، آدرس پایان محدوده IPهای قابل تخصیص را وارد نمایید. توجه نمایید که محدوده وارد شده، بایستی در محدوده آدرس شبکه شما باشد.

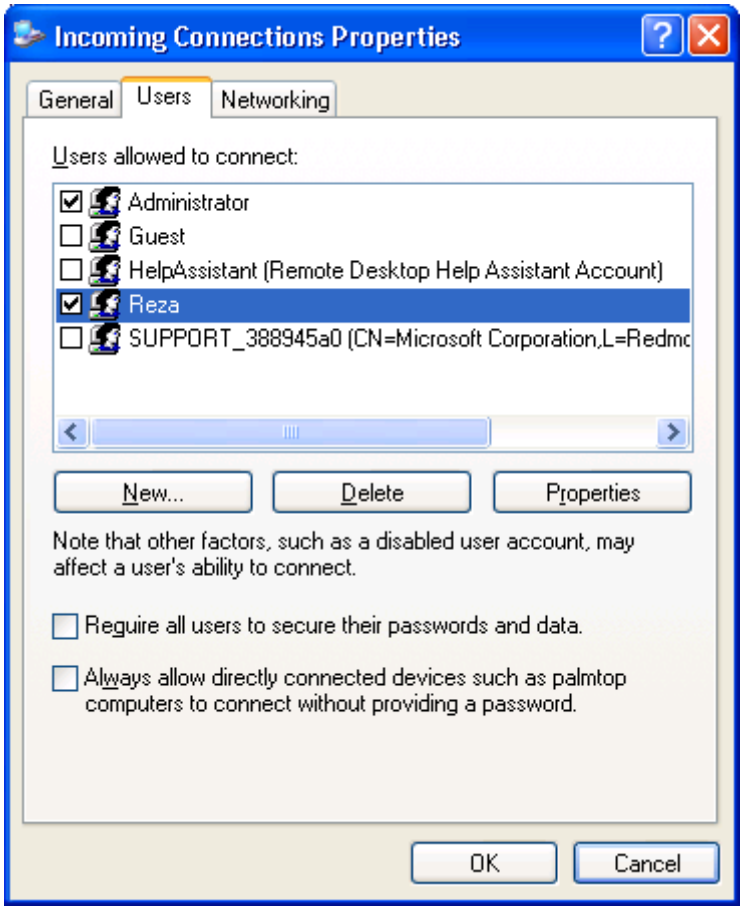


در نهایت روی دکمه Finish کلیک نمایید.

با انجام این کار، در Control Panel ➔ Network Connections، یک آیکون بـه نـام Incoming Connections سـاخته مـی شود. برای انجام تنظیمات، روی آن راست کلیک کرده و گزینه Properties را انتخاب نمایید.

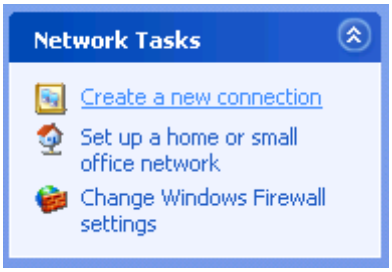


مثلاً با ورود به سربرگ Users، توانایی تعیین کاربرانی که قابلیت اتصال از راه دور را دارند، را پیدا می کنید.



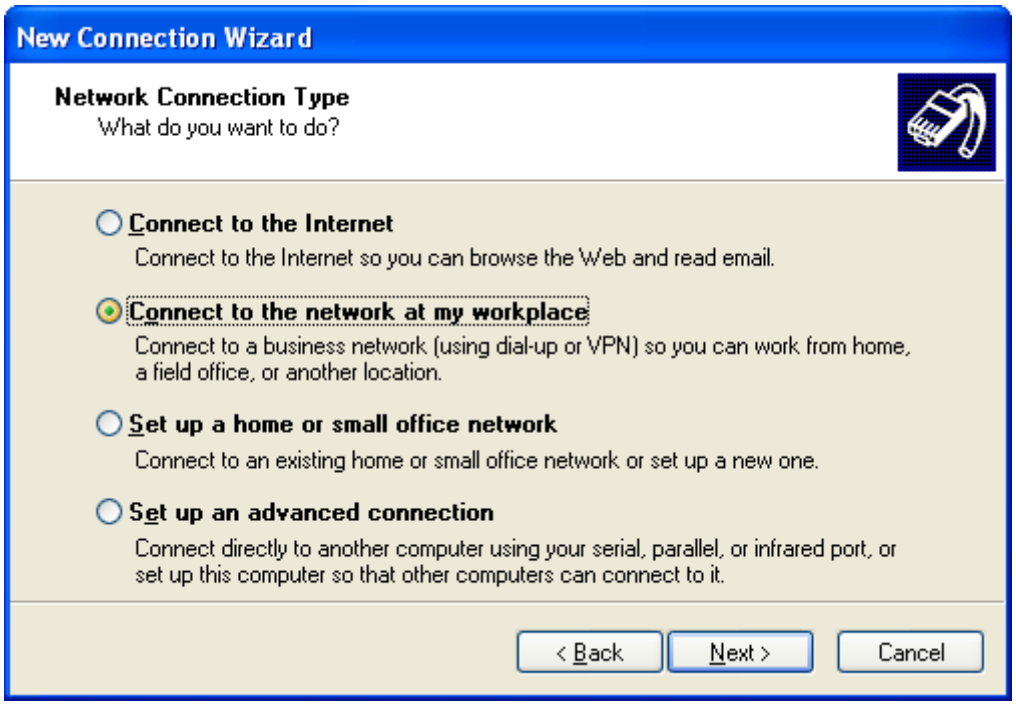
۲۵-۵- اتصال به کامپیوتر راه دور توسط Dial up یا VPDN

برای انجام این کار، در کامپیوتر مبدا ابتدا بایستی یک Connection بسازید. بدین منظور، وارد Control Panel ➔ Network Connections شده و روی قسمت Create a new connection کلیک کنید.



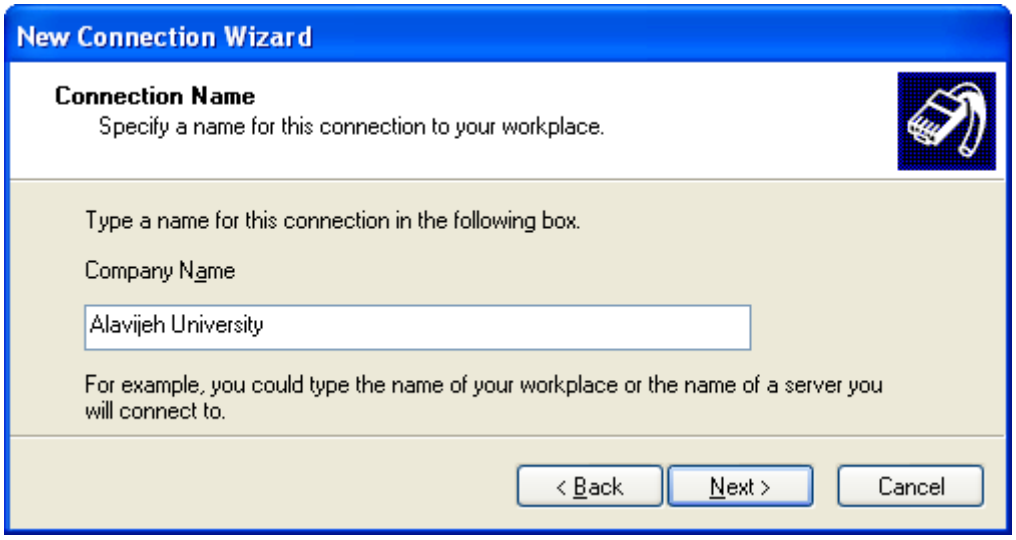
در صفحه خوش آمد گویی، روی دکمه Next کلیک کنید.

سپس گزینه Connect to the network at my workplace را انتخاب کرده و سپس Next را بزنید.

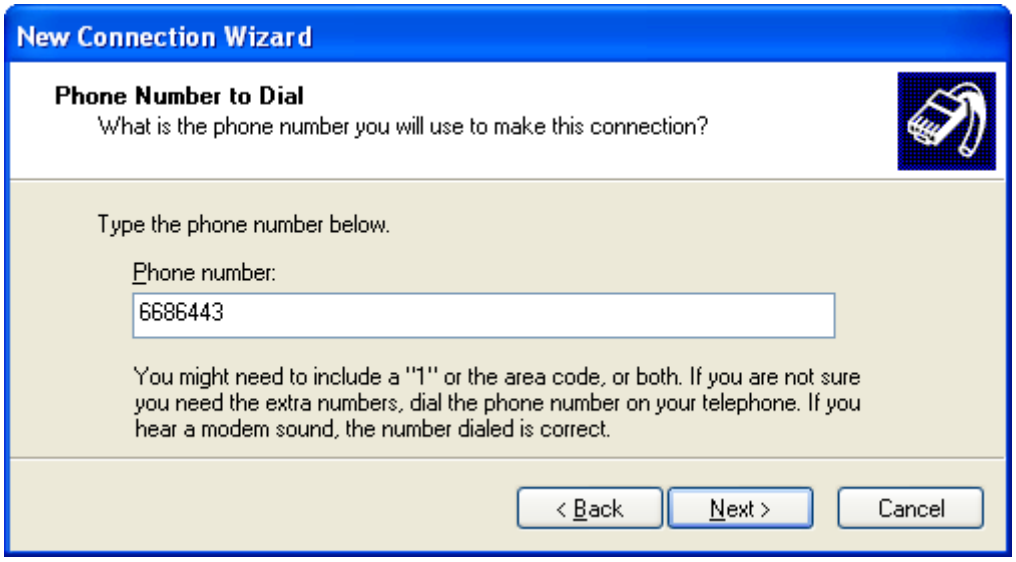


در این صفحه دو گزینه وجود دارد. گزینه اول برای VPDN و گزینه دوم برای VPN است. گزینه دوم را بعدا توضیح می دهید. در این قسمت گزینه Dial up connection را انتخاب کرده و Next را بزنید.

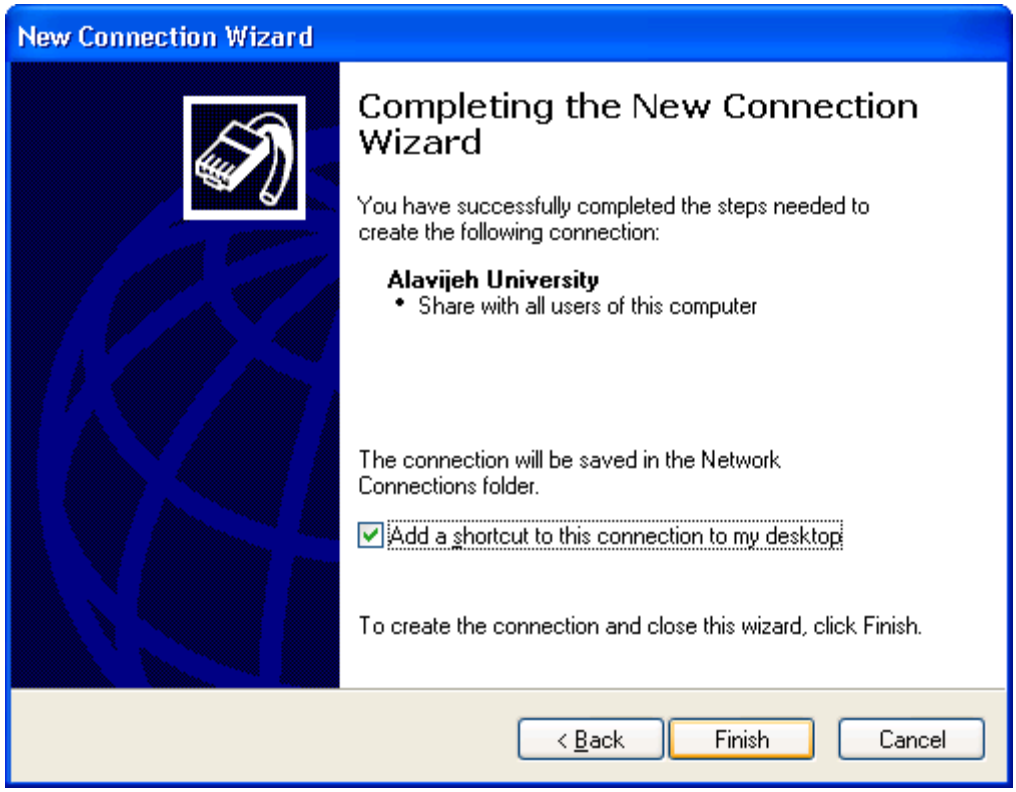
در صفحه بعد، نامی برای اتصال خود انتخاب کنید.



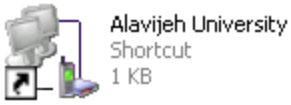
در صفحه بعد، شماره تلفن کامپیوتری که می خواهید به آن شماره گیری کنید را وارد نمایید. کامپیوتر مقصد بایستی توسط یک مودم Dial up به خط تلفن متصل باشد. توجه نمایید که اگر مقصد تماس درون شهری است، فقط شماره مقصد (مثلاً ۶۶۸۶۴۴۳)، اگر بین شهری است، علاوه بر شماره تلفن، کد شهر نیز نیاز است (مثلاً ۰۳۱۱۶۶۸۶۴۴۳). و اگر مقصد بین دو کشور جدا است، هم کد کشور، هم کد شهر و هم شماره تلفن مقصد مورد نیاز است (مثلاً ۹۸۳۱۱۶۶۸۶۴۴۳+ یا ۰۰۹۸۳۱۱۶۶۸۶۴۴۳).



در نهایت گزینه Add a shortcut to this connection to my desktop را انتخاب کرده و روی Finish کلیک کنید.

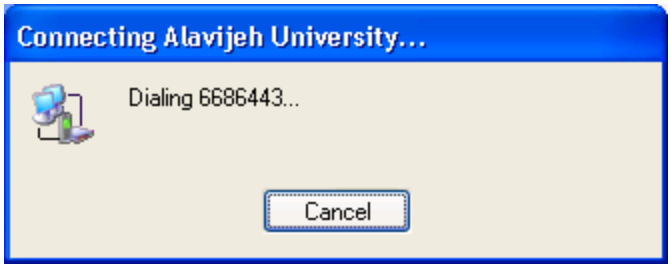


با این کار، یک آیکون در Network Connections و صفحه دسکتاپ شما ساخته می شود. برای اتصال آن را باز نمایید.



در صفحه باز شده، در قسمت User Name، نام کاربری و در قسمت Password، رمز عبور خود را وارد نمایید. توجه نمایید که جهت احراز هویت، این نام کاربری و رمز عبور، بایستی در کامپیوتر مقصد ثبت شده باشد. در نهایت در قسمت Dial شماره مقصد را وارد کرده (به طور پیش فرض این قسمت پر است)، و روی دکمه Dial کلیک نمایید.

با این کار سیستم شروع به شماره گیری می کند. در صورت تایید کامپیوتر مقصد، به آن متصل خواهید شد.

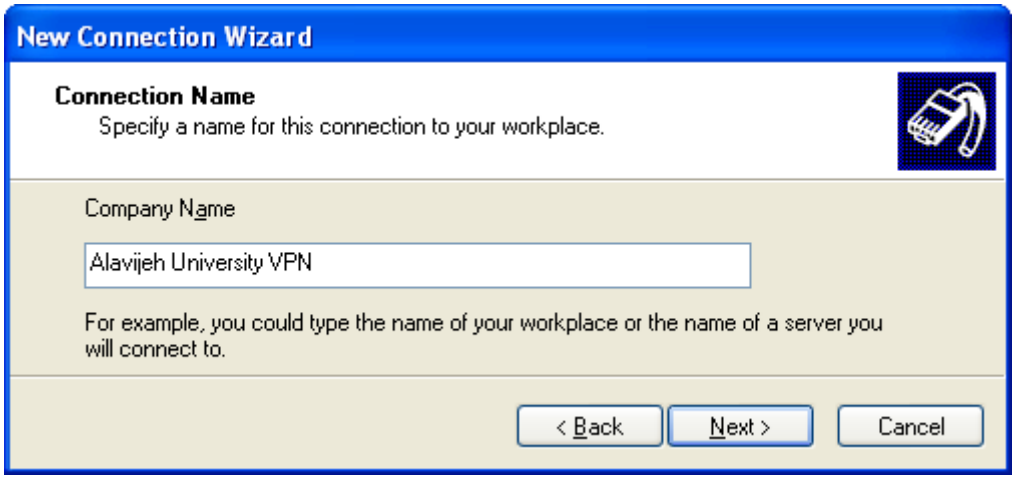


حال می توانید با اعضای شبکه ارتباط برقرار کنید (مثلاً توسط نرم افزار Netmeeting)، یا بـه کمـک Remote Desktop مـی توانید یکی از کامپیوتر ها را کنترل نمایید.

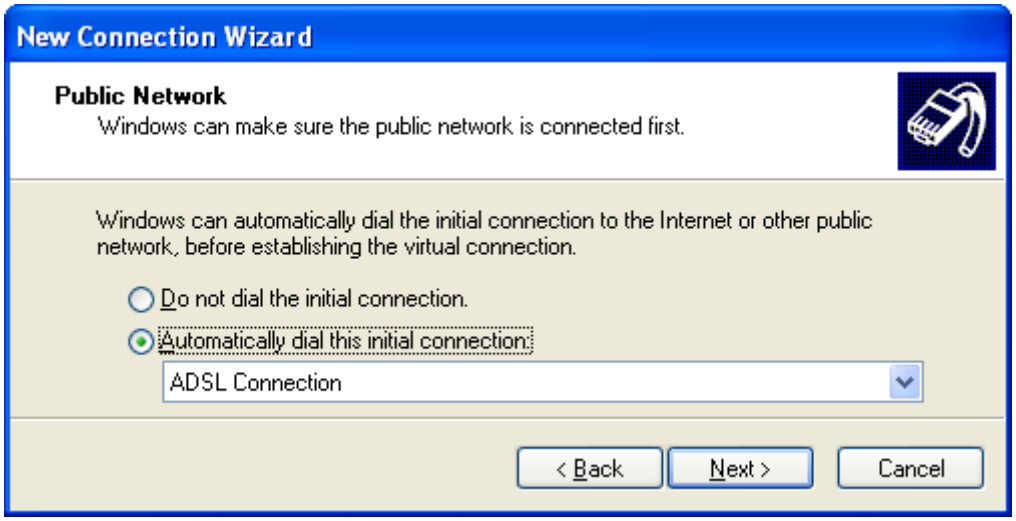
۲۵-۶- اتصال به کامپیوتر راه دور توسط VPN

در قسمت های قبل گفتیم که اتصال توسط VPDN به علت هزینه های تلفن، مقرون به صرفه نیست. لذا از روش دیگری بـه نام VPN استفاده می کنیم. بدین منظور، در قسمت قبل هنگام ساخت Connection، به صفحه ای مانند زیر برخورد کـردیم. این بار گزینه Virtual Private Network Connections را انتخاب کرده و روی Next کلیک کنید.

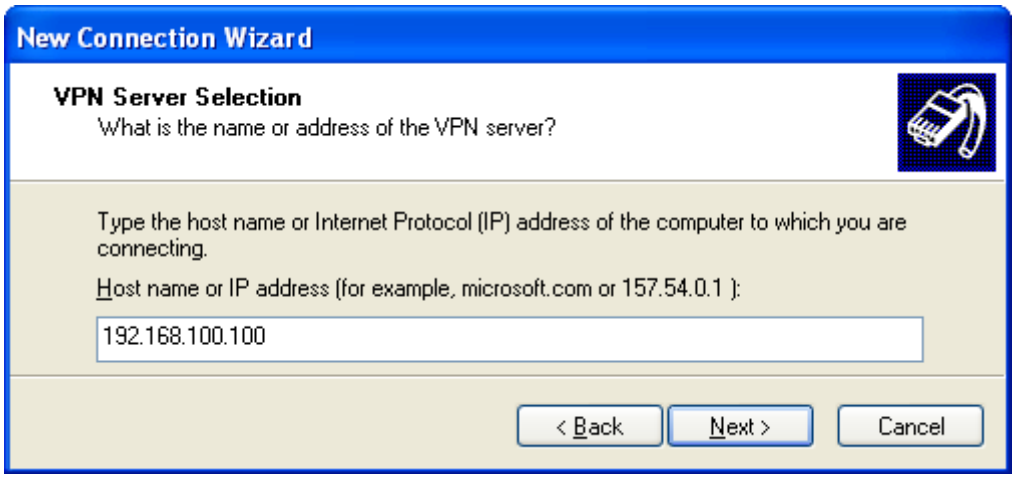
در صفحه بعد، یک نام برای Connection خود وارد نمایید.



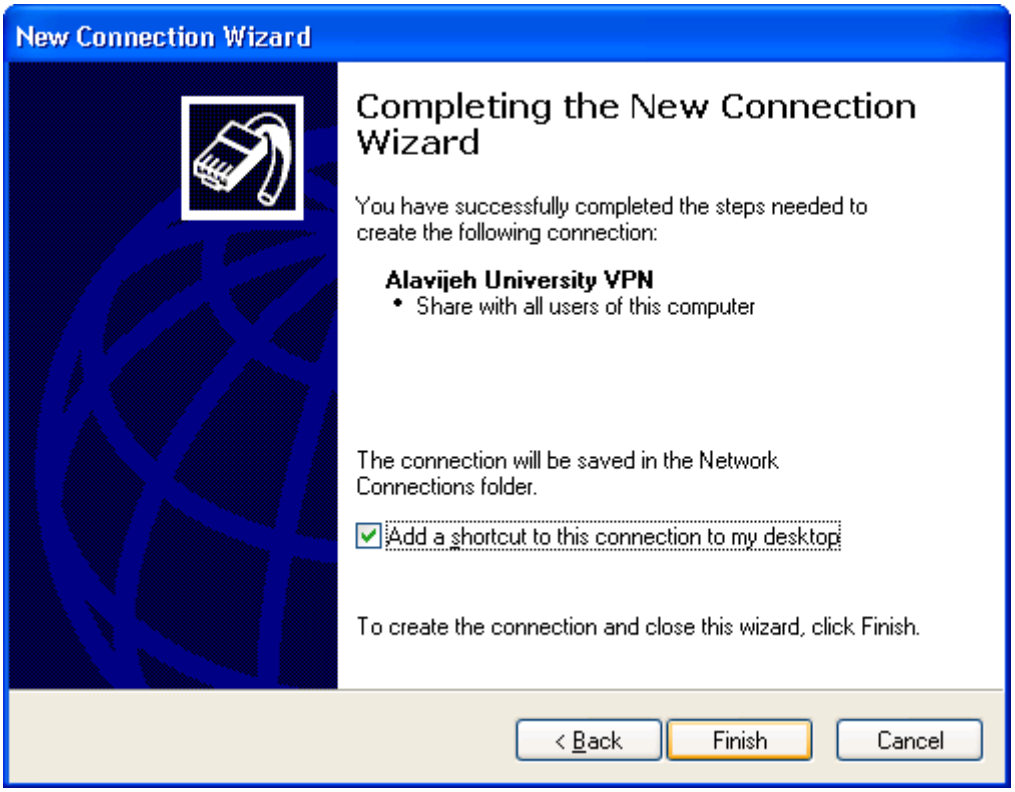
لازمه استفاده از VPN این است که سیستم مبدا و مقصد هر دو به اینترنت متصل باشند. در این صفحه مشخص می نمایید که هنگام استفاده از VPN، اگر سیستم شما به اینترنت متصل نبود، توسط کدام Connection به اینترنت وصل می شوید؟ مزیت این قسمت این است که می تواند یک اتصال ADSL را انتخاب نمایید.



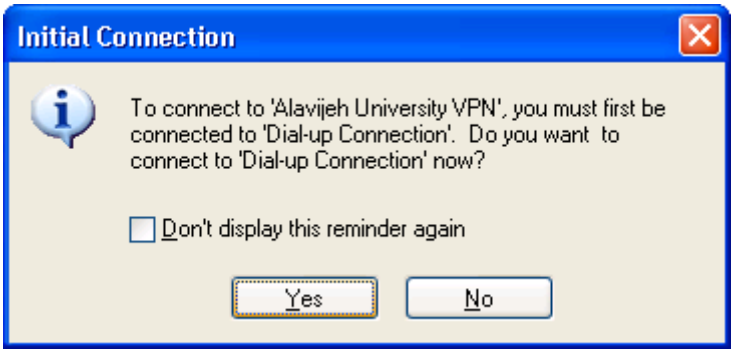
در صفحه بعد، آدرس IP کامپیوتر مقصد را وارد نمایید. همانطور که گفتیم، اتصال با VPN به کمک آدرس IP است. توجه نمایید که اگر کامپیوتر مقصد Static IP ندارد و هر بار هنگام اتصال به اینترنت، آدرس IP آن عوض می شود، شما نیز بایستی هر بار تنظیمات IP مربوط به Connection خود را تغییر دهید. در مورد تنظیمات جلوتر بحث می کنیم.



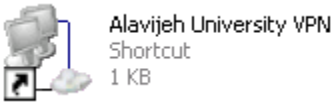
در نهایت گزینه Add a shortcut to this connection to my desktop را انتخاب کرده و روی Finish کلیک کنید.



پس از ساخت Connection، سیستم به شما پیغام می دهد که برای استفاده از VPN، بایستی ابتدا به اینترنت متصل شوید و از شما می پرسد که آیا می خواهد با Connectionی که مشخص کرده اید به اینترنت متصل شود؟ فعلا No را انتخاب کنید.



پس از پایان ساخت، یک آیکون در Network Connections و صفحه دسکتاپ شما ساخته می شود. برای اتصال آن را باز نمایید.



در صفحه باز شده، در قسمت User Name، نام کاربری و در قسمت Password، رمز عبور خود را وارد نمایید. توجه نمایید که جهت احراز هویت، این نام کاربری و رمز عبور، بایستی در کامپیوتر مقصد ثبت شده باشد. در نهایت برای اتصال روی دکمه Connect کلیک نمایید. همچنین اگر می خواهید تنظیماتی را انجام دهید، روی دکمه Properties کلیک نمایید.

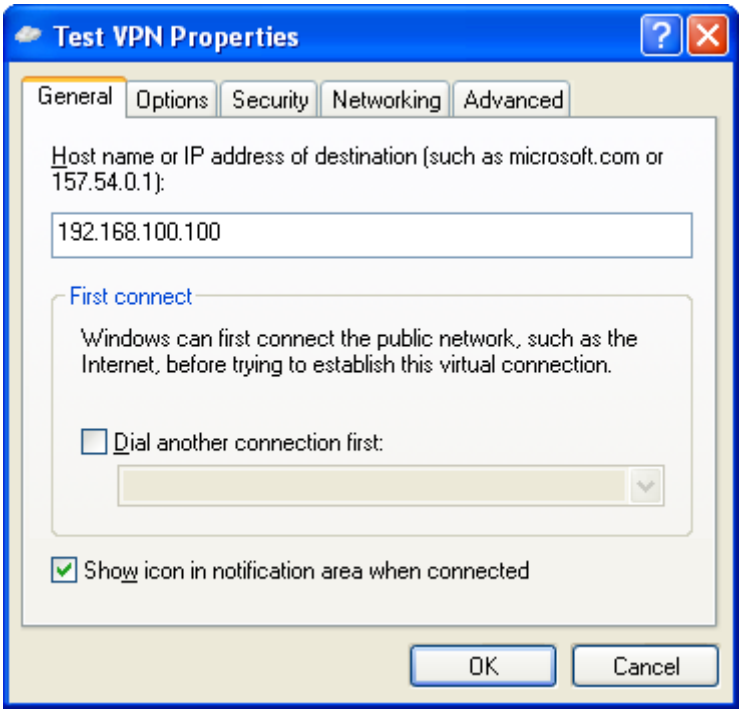
سربرگ General

همانطور که در شکل زیر ملاحظه می کنید، این قسمت نیاز به تنظیمات و تغییرات چندانی ندارد. اگر می خواهید نام و یا آدرس IP سروری که می خواهید به آن وصل شوید را تغییر دهید، در اولین کادر می توانید تغییرات را وارد نمایید. توجه نمایید که ما آدرس IP مورد نظر را قبلاً وارد کرده بودیم.

همچنین در همین صفحه و در قسمت First Connection می توانید تنظیم کنید که کدام یک از خطوط ISP را برای برقراری اتصال اینترنتی به VPN سرور می خواهید استفاده نمایید. این گزینه را نیز قبلاً تنظیم نموده ایم.

توجه: اگر بخواهید به VPN سرور داخل شبکه متصل شوید نیازی به تعریف این گزینه نیست.

در انتها نیز گزینه ای مربوط به فعال یا غیر فعال کردن نمایش آیکون آداپتور شبکه در System Tray (بعد از برقراری اتصال به شبکه) می باشد.



سربرگ Options

همانطور که در شکل زیر مشاهده می نمایید، در این قسمت عملیاتی که در هنگامی برقراری اتصال انجام می شود، را می توان تنظیم نمود. برخی از این تنظیمات در قالب سوال های زیر نشان داده شده است.

- آیا سیستم وضعیت اتصال را به شما نشان دهد یا خیر؟
- نام کاربری، کلمه عبور و نام Domain را درخواست کند یا خیر؟

و با گزینه هایی که در قسمت Redialing Options وجود دارد، عکس العمل سیستم در مقابل عدم دریافت پاسخ از طرف سرور، را می توانید تنظیم نمایید:

- در صورت عدم دریافت پاسخ از سرور، چند بار سعی برای اتصال صورت گیرد؟
- تنظیم فاصله زمانی بین هر سعی با سعی دیگر
- اگر اتصال ناخواسته قطع شد، آیا مجددا برقرار شود یا خیر؟

در حالت عادی نیازی به تغییر در این برگه نیست.

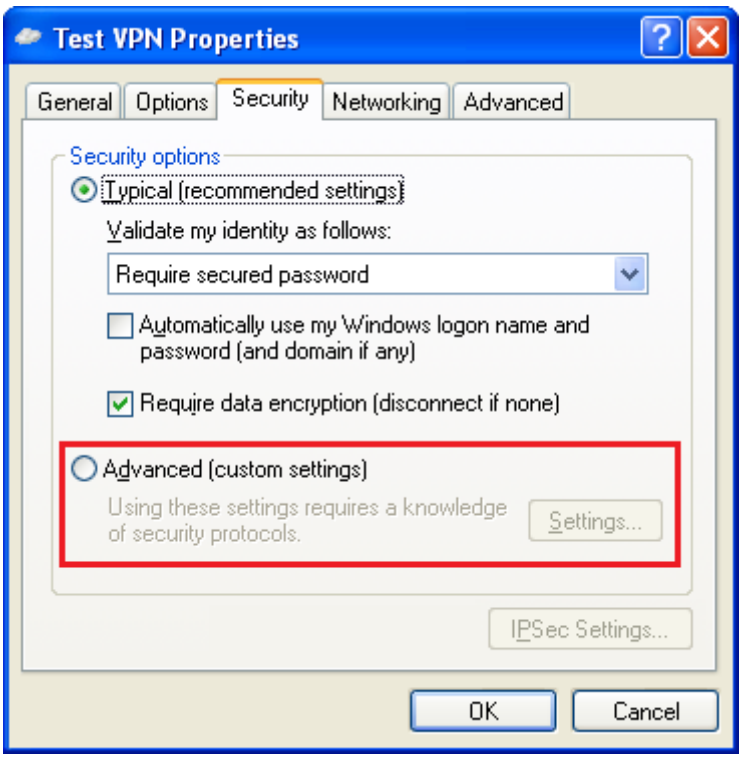
سربرگ Security

همانطور که در شکل زیر می بینید، در این قسمت می توانید امنیت اتصال خود را تنظیم کنید. اگر طبق دستور العمل های داده شده در VPN Server تنظیمات را انجام داده باشید نیازی به تغییر در اینجا احساس نمی شود، مگر اینکه بخواهید امنیت بیشتری را در نظر بگیرید. برای انجام این کار گزینه Advanced را انتخاب نموده و سایر تنظیمات را برحسب نیاز انجام دهید. (توضیحات تک تک گزینه های آن خارج ار بحث این جزوه می باشد).

توجه: این گزینه زیر را **فعال نکنید**:

Automatically use my Windows logon name and password

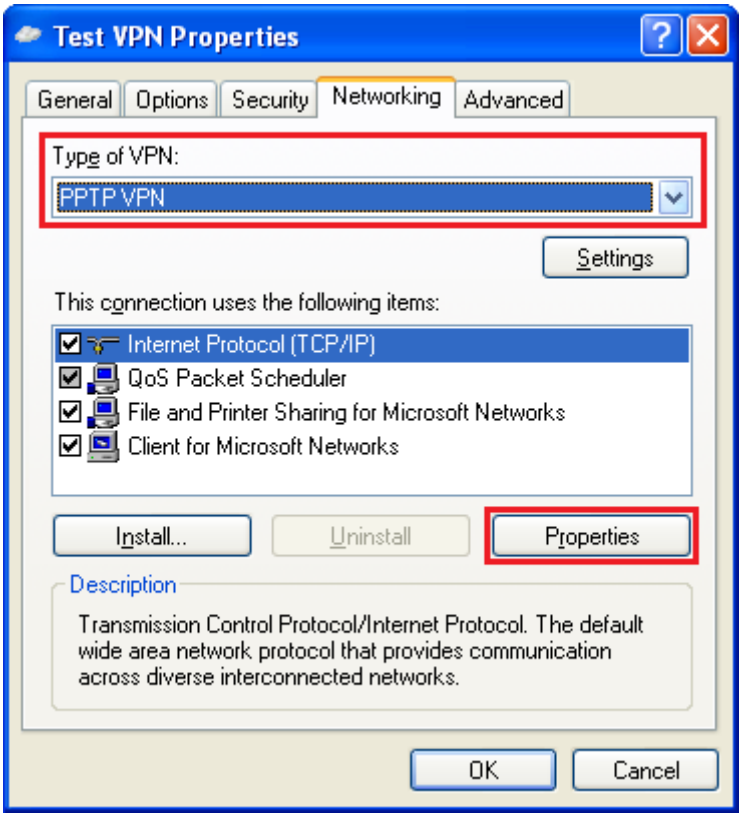
اگر این گزینه در کامپیوتر فعال باشد و این کاربر به قصد استراحت، برای مدت کوتاهی کامپیوتر را رها کرده باشد، هر کسی می تواند از طریق این کامپیوتر به شبکه (VPN Server) وصل شود. زیرا با فعال کردن این گزینه عملاً نیاز به تایپ نام کاربری و کلمه عبور برای ورود به سرور را از بین برده اید.



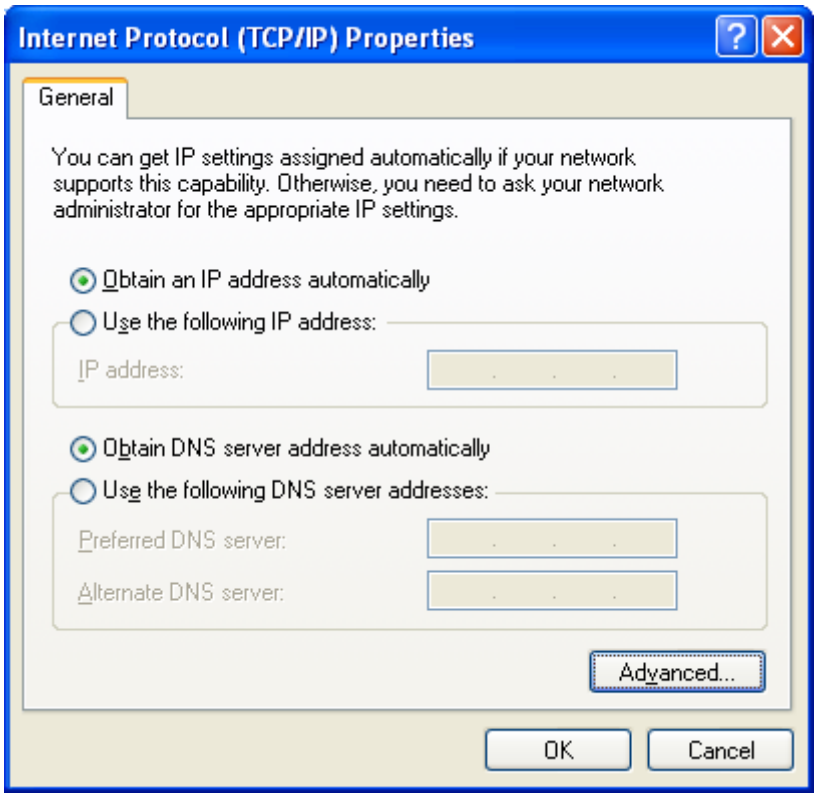
سربرگ Networking

در این قسمت تنظیمات مختلفی می توان انجام داد. همانگونه که در شکل زیر می بینید، اولین تنظیم مربوط بـه نـوع اتصـال VPN شما می باشد. به صورت پیش فرض Automatic انتخاب شده است که هر دو حالت PPTP VPN و L2TP VPN را بـه ترتیب بررسی می نماید.

PPTP برای کاربردهای عمومی و غیر حرفه ای مناسب تر می باشد. پروتکل L2TP که به وسیله شـرکت CISCO ارائـه شـده است به لحاظ امنیتی بسیار قدرتمندتر است. پروتکل دیگری به نام IPSec پایه ریزی شده است کـه پیچیـدگی هـای خاصـی دارد. ما در اینجا از پروتکـل PPTP اسـتفاده مـی کنـیم کـه تنظیمـات راحـت تـری دارد. PPTP مخفـف Point-To-Point Tunneling Protocol است.



یکی دیگر از تنظیمات، تعیین این است آیا می خواهید برای اتصال به شبکه VPN از Default Gateway استفاده شود یا نه؟ برای این کار می توانید، با توجه به شکل فوق، پس از انتخاب Internet Protocol (TCP/IP) دکمه Properties را بزنید. در صفحه باز شده، روی Advanced کلیک کنید.



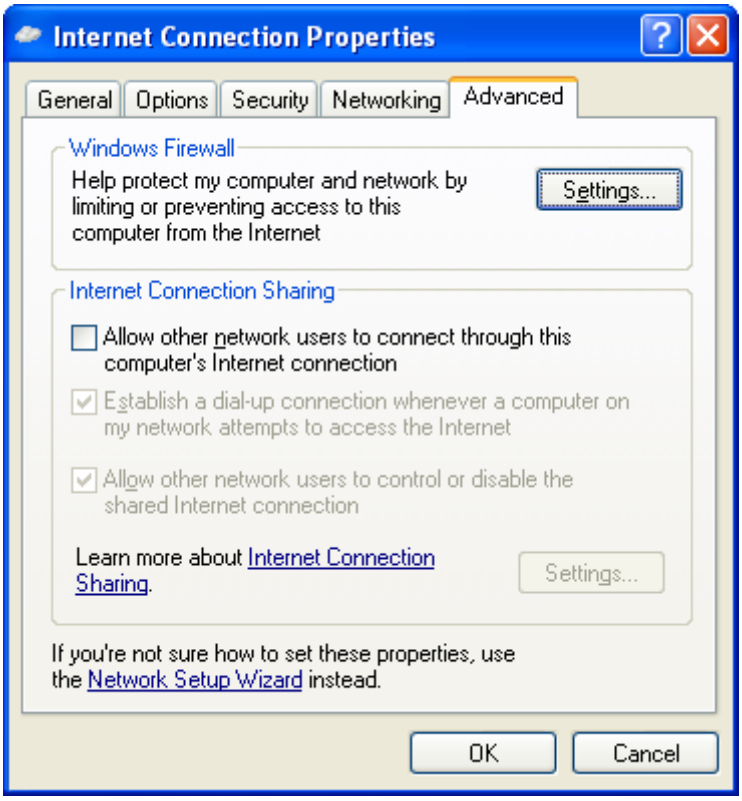
در این صفحه، گزینه Use default Gateway on remote network به صورت پیش فرض تیک خورده و فعال است. ممکن است که برایتان این سوال پیش بیاید که چه زمانی این گزینه فعال و چه زمانی غیر فعال کنیم؟

بعضی از کاربران در خانه، و یا بعضی ها در کافی نت ها و یا هتل و غیره... و از راه اینترنت به VPN وصل می شوند. اینگونه افراد برای اتصال به شبکه VPN، در واقع از راه دور (Remote) به VPN Server وصل می شوند. بنابرین با فعال کردن این گزینه یک مسیری برای آنها ایجاد کرده اید که بتوانند بدون مشکل وصل شوند.

توجه: برای کاربران داخلی (کاربران داخل شبکه) که از یک محدوده خاصی از IP آدرس استفاده می کنند، گزینه " Use default Gateway on remote network" را غیر فعال کنید.

سربرگ Advanced

در اتصال معمولی و ساده به شبکه VPN، این قسمت نیاز به تنظیمات خاصی ندارد. در این صفحه امکان انجام تنظیمات امنیتی و به اشتراک گذاری اتصالات اینترنت وجود دارد.

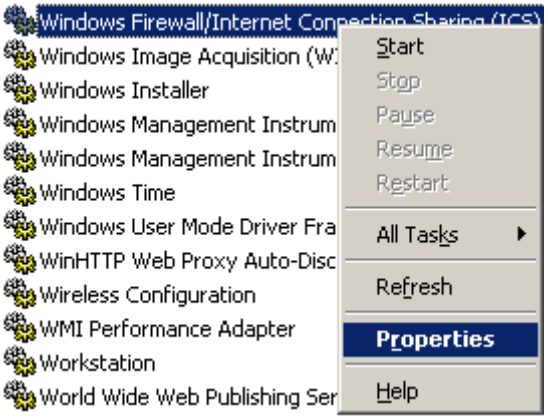


بعد از انجام تنظیمات لازم، نوبت به برقراری ارتباط می رسد. دکمه Connect در پنجره اصلی را بزنید. چنانچه تنظیمات VPN Server و VPN Client را به درستی انجام داده باشید. اتصال با موفقیت انجام می شود و آیکونی مشابه آیکون اتصال به اینترنت در System Tray ظاهر می شود. که می توانید خصوصیات اتصال خود را با زدن دکمه Properties مشاهده کنید. با این اتصال مانند آن است که خود در سرور قرار گرفته باشید. و از امکانات آن استفاده نمایید.

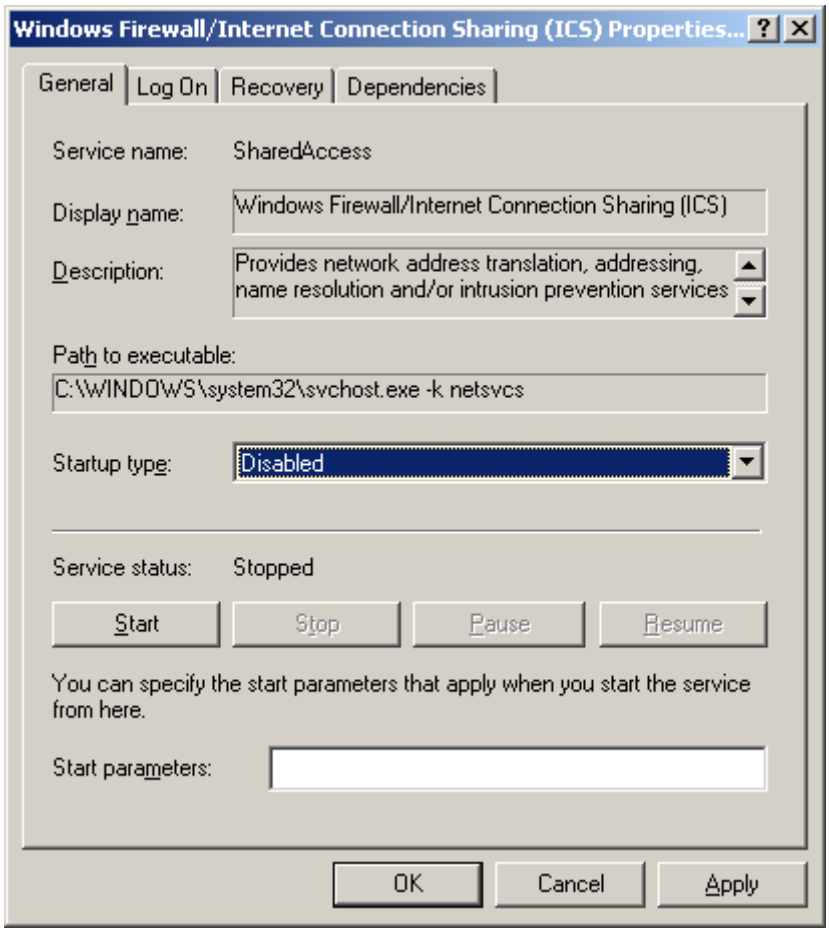
۲۵-۷- نصب VPN Server روی ویندوز سرور

۲۵-۷-۱- غیر فعال کردن Service

برای راه اندازی VPN Server، ابتدا بایستی سرویس Windows Firewall/Internet Connection Sharing را غیر فعال کنید. بدین منظور ابتدا وارد Control Panel ➔ Administrative Tools ➔ Services شده، روی سرویس مذکور راست کلیک کرده و سپس گزینه Properties را انتخاب نمایید.



سپس در قسمت Startup type، گزینه Disabled را انتخاب کنید. همچنین با کلیک روی دکمه Stop، سرویس مذکور را غیر فعال نمایید. در نهایت روی OK کلیک کنید.



۲۵-۷-۲- نصب VPN Server

برای اعطای نقش Remote Access/VPN Server به ویندوز سرور ۲۰۰۳ یا به عبارت دیگر برای نصب و راه اندازی VPN Server باید ویزارد Configure Your Server Wizard را از مسیر زیر احضار کنیم:

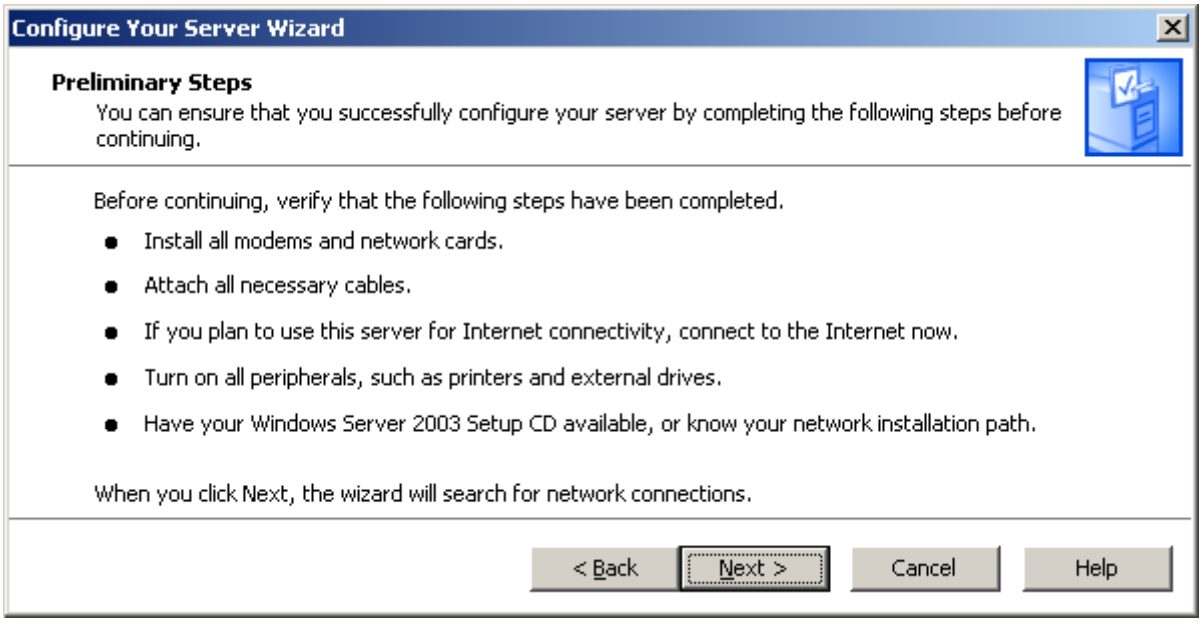
Start ➔ Administrative Tools ➔ Configure Your Server Wizard

اولین پنجره ای که ظاهر می شود، اطلاعات اولیه ای در مورد این ویزارد را نشان می دهد.

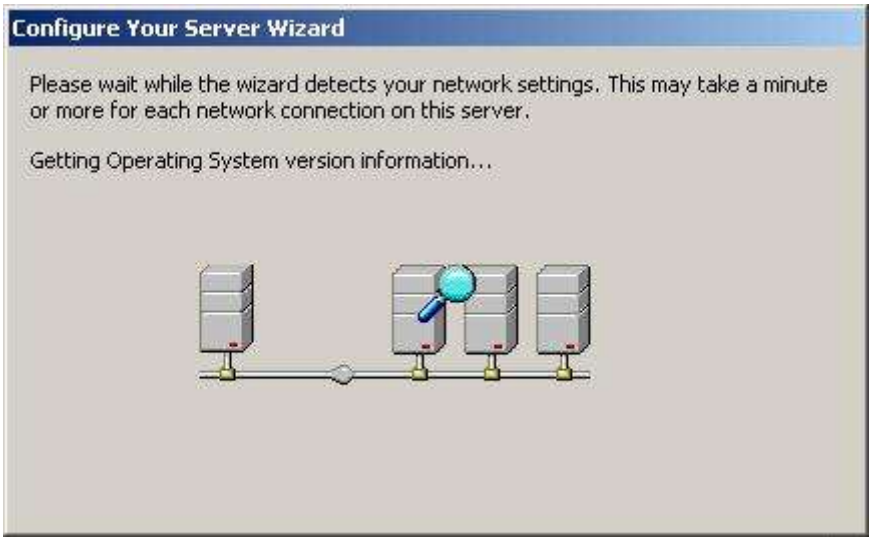
پنجره Preliminary Steps مواردی که لازم است قبل از شروع ویزارد انجام دهید را باز گو می کند مثلاً:

- اطمینان از نصب مودم ها و کارت های شبکه
- اگر ویزارد را برای اتصال به اینترنت می خواهید، از اتصال خود به اینترنت اطمینان حاصل کنید.
- و یا اینکه CD نصب ویندوز را آماده داشته باشید و غیره....

در این صفحه، روی دکمه Next کلیک کنید.



این صفحه نیز به صورت خودکار بسته خواهد شد.



پنجره Server Role سومین پنجره ای است که ظاهر می شود. همانطور که در شکل زیر مشاهده می کنید، لیستی از نقش هایی که روی سیستم می توانید اعمال کنید نشان داده شده است که در ستون مقابل هر کدام، وضعیت آن Role را از لحاظ اینکه این نقش اعطا شده است یا نه نشان داده شده است. برای اعطای نقش Remote Access / VPN به ویندوز، این مورد را از لیست انتخاب کرده و دکمه Next را بزنید.

Server Role	Configured
File server	Yes
Print server	No
Application server (IIS, ASP.NET)	Yes
Mail server (POP3, SMTP)	Yes
Terminal server	No
Remote access / VPN server	No
Domain Controller (Active Directory)	Yes
DNS server	Yes
DHCP server	No
Streaming media server	No
WINS server	No

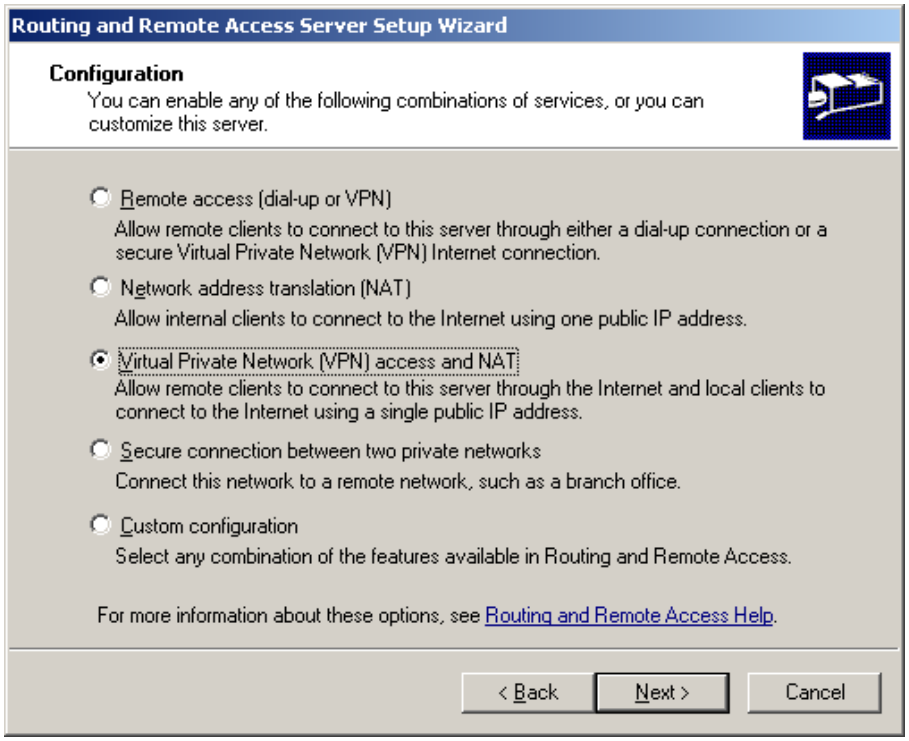
پنجره بعدی ویزارد، توضیح مختصری درباره این نقش میدهد. پس از مطالعه آن دکمه Next را بزنید.

ویزاردی با نام Routing and Remote Access Wizard ظاهر می شود (ویزارد RRAS) که در ادامه به آن اشاره می شود.

۲۵-۷-۳- تنظیمات Routing and Remote Access (ویزارد RRAS)

مانند تمام ویزارد ها، اولین پنجره این ویزارد، توضیح و نکات مختصری راجع به آن می باشد که ما با مطالعه آن و زدن دکمه Next از آن می گذریم.

در پنجره بعدی یعنی پنجره Configuration، گزینه های مختلفی وجود دارد که با توجه به نوع اتصال از راه دور (Remote Access Connection) یکی از گزینه ها را انتخاب می کنیم. و چون قصد ما در اینجا راه اندازی VPN بر اساس PPTP می باشد ما گزینه Virtual Private Network VPN and NAT را انتخاب کرده و Next می زنیم.

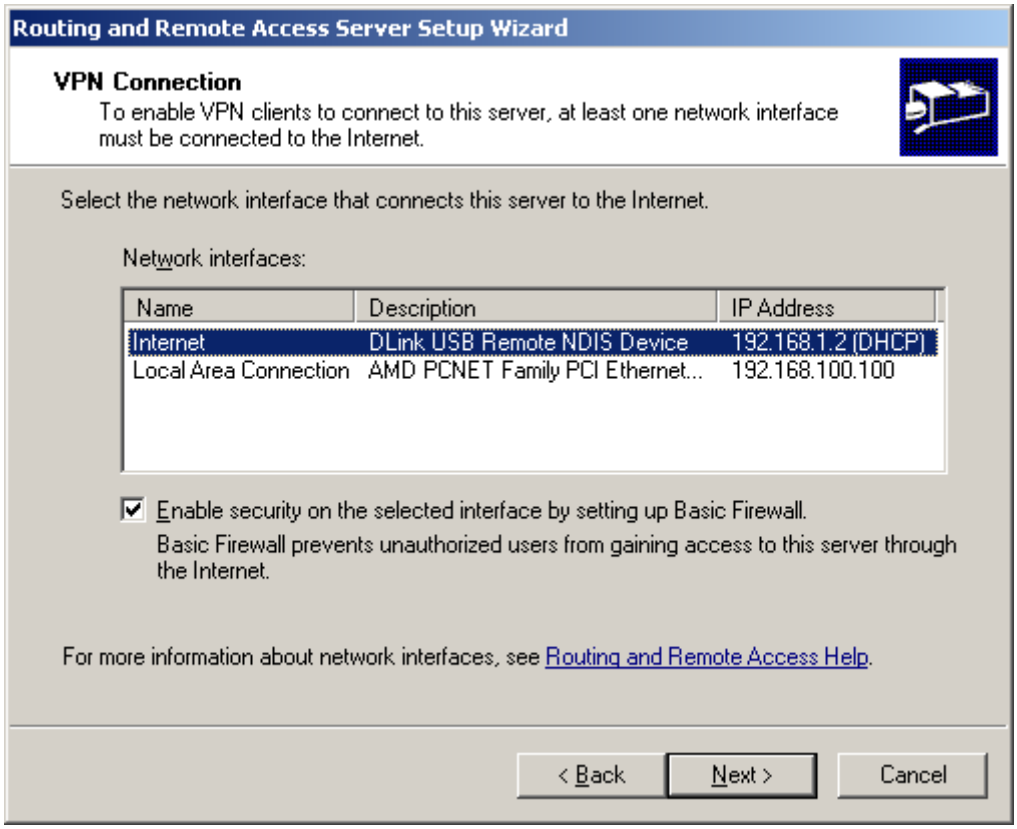


توجه نمایید که برای راه اندازی VPN Server، حداقل به دو کارت شبکه نیاز دارید. یکی برای اتصال به اینترنت و دیگری برای اتصال به شبکه محلی. در غیر اینصورت، قادر به نصب VPN Server نخواهید بود.

مطابق شکل زیر و در پنجره VPN Connection **باید آداپتور یا Deviceی که با آن به اینترنت وصل می شوید را تعیین کنید.** نکته ای که در اینجا قابل توجه می باشد این است که برای برقراری امنیت بیشتر و در واقع برای کنترل دقیق تر، بهتر است که کارت شبکه مستقلی را برای VPN Server در نظر بگیرید. که در اینجا ما کارتی غیر از کارت شبکه ای که برای اتصال کاربران محلی انتخاب می کنیم.

گزینه Enable security on the selected interface by setting up Basic Firewall را تیک بزنید. این گزینه به عنوان یک Firewall نرم افزاری فعال شده و سرور شما از نفوذ خرابکاران و حملات مخرب آنها از راه اینترنت در امان نگه می دارد. هر

چند، نصب فایروال های پیشرفته و مستقل و یا یک فایروال سخت افزاری برای شبکه های محرمانه ضروری می باشد (و این بستگی به درجه اهمیت شبکه و اطلاعات موجود در آن دارد).



مطابق شکل زیر، باید تنظیم نمایید که از کدام کارت شبکه برای کاربران محلی شبکه استفاده می کنید. اگر دو کارت شبکه بیشتر نداشته باشید، شکل زیر را مشاهده نخواهید نمود؛ زیرا یک کارت شبکه برای اینترنت و دیگری برای سرویس دهی به کاربران VPN استفاده می شود.

همانطور که یک کاربر محلی برای برقراری اتصال با سرور و سایر کلاینت های موجود در شبکه نیاز به داشتن یک IP Address در همان محدوده دارد (یعنی باید قسمت Net ID آدرس های IP آن ها یکسان باشد)، VPN Clientها نیز در هنگام برقراری اتصال به VPN Server، نیاز به یک IP Address دارند که بتوانند به منابع مجاز در سرور دسترسی داشته باشند. در اینجا شما به عنوان مدیر شبکه با انتخاب یک روش از دو راه موجود، نحوه واگذاری آدرس IP به کلاینت های VPN را تعریف می کنید.

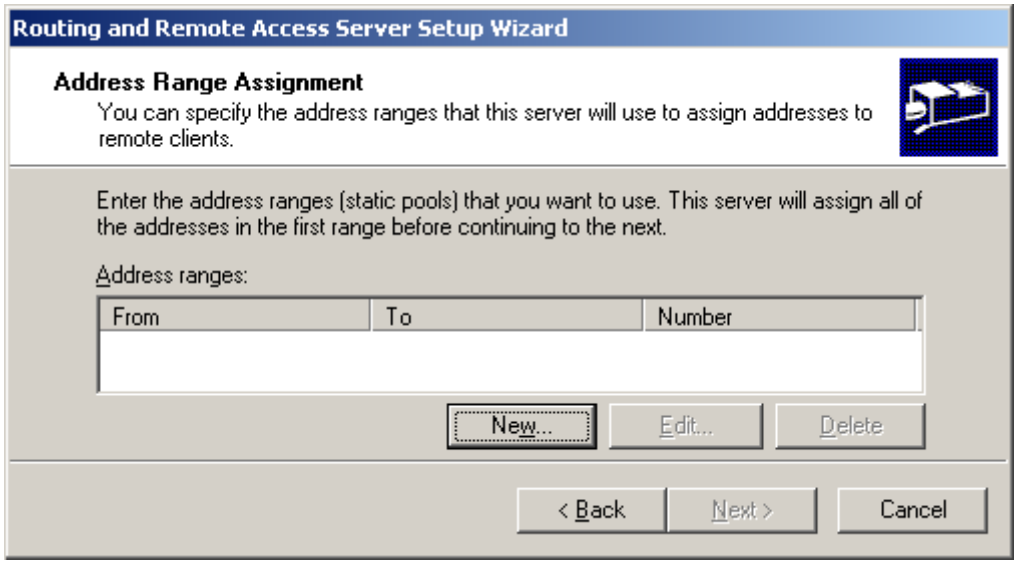
۱. با نصب و تعریف DHCP که در فصول قبل توضیح داده شد و اعمال تنظیمات لازم، سرور خود را به عنوان DHCP Server تعریف می کنید، به طوری که کاربران در هنگام برقراری اتصال به سرور شما از محدوده IP هایی که در سرور تعریف کرده اید، یکی را به خود اختصاص می دهند. با انتخاب گزینه Automatically روند واگذاری IP آدرس از روی تنظیمات DHCP Server انجام می گیرد.

۲. تعیین محدوده خاصی از IP آدرس هایی که به کاربران واگذار شود.

ما در اینجا گزینه دوم را انتخاب می کنیم. به این دلیل که می خواهیم با استفاده از محدوده خاصی از IP آدرس ها که انتخاب می کنیم، کاربران شبکه محلی که به سرور وصل می شوند را از کاربرانی که از اینترنت (VPN Client) وصل می شوند تشخیص دهیم.

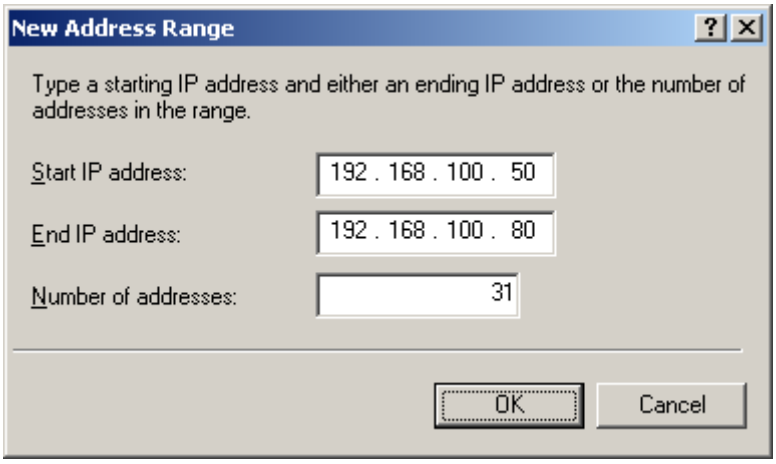
پس از انتخاب گزینه دوم (یعنی From a specified range of addresses)، دقیقا تعریف می کنید که چه آدرس IPهایی را به VPN Server اختصاص می دهید که سرور به Client ها واگذار نماید.

برای اینکار دکمه New در پنجره Address Range Assignment را بزنید.



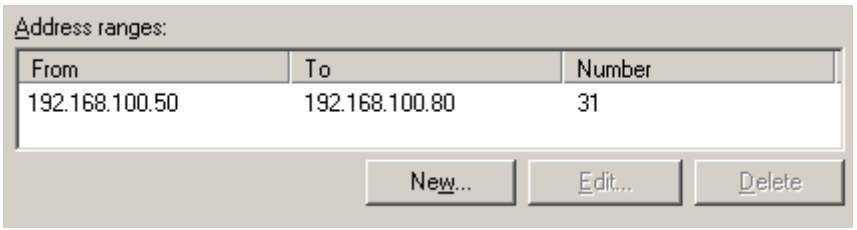
در پنجره باز شده، محدوده اولین و آخرین آدرس IP را تعیین کنید. بدین ترتیب، کاربران پس از اتصال به سرور به کمک VPN، یکی از آدرس های موجود در این محدوده را دریافت می کنند.

فیلد Number of addresses به صورت اتوماتیک با توجه به محدوده انتخابی شما تعیین می شود. می توانید فقط اولین آدرس IP را بنویسید و تعداد آدرس IPها را مشخص کنید؛ ویزارد محاسبات را انجام داده و آدرس IP پایانی را خودش وارد می کند. دکمه OK را بزنید تا تنظیمات شما ثبت شود.

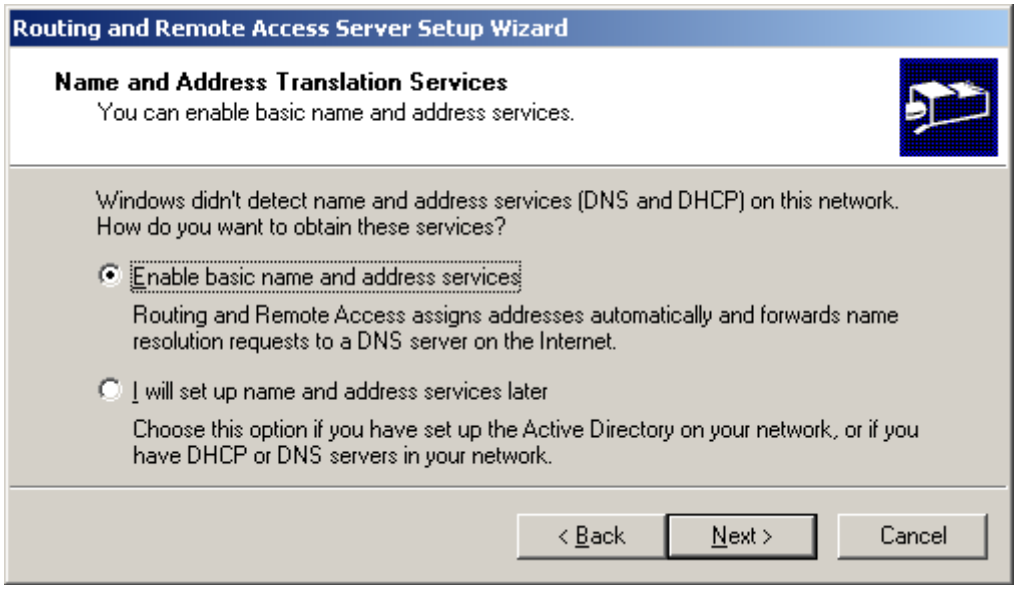


نکته مهم: دقت فرمایید که محدوده آدرس وارد شده، تداخلی با آدرس کامپیوتر هایی که اکنون به صورت محلی با کامپیوتر سرور شبکه هستند، نداشته باشد.

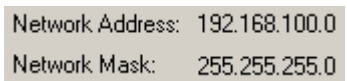
بدین ترتیب، محدوده وارد شده به لیست محدوده های آدرس IP اضافه می شود.



در مرحله بعدی، سیستم بررسی می نماید تا ببیند که آیا DNS Server و DHCP Server در شبکه شما وجود دارد یا خیر؟ اگر وجود نداشته باشد، صفحه زیر نشان داده می شود. با انتخاب گزینه اول، می توان این سرویس ها را نصب نمود. با انتخاب گزینه دوم، به سرور می گوییم که این تنظیمات را بعدا به صورت دستی انجام خواهیم داد.



در پنجره بعدی، آدرس شبکه مجازی که به وجود خواهد آمد را مشاهده خواهید نمود.



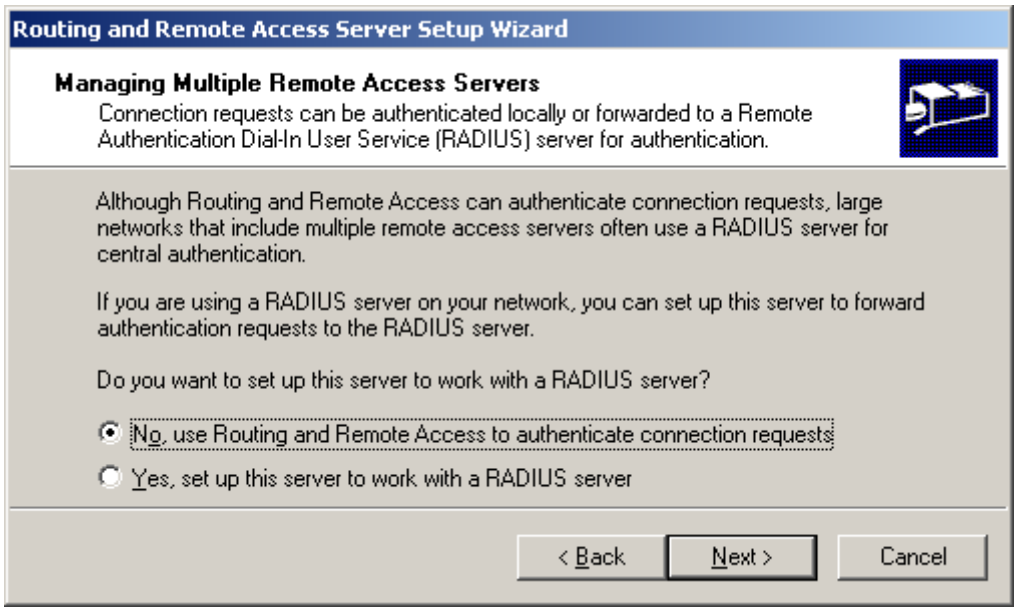
در پنجره بعدی اطلاعات اعتبار سنجی را مشاهده خواهید نمود. اعتبار سنجی (Authentication) یا بازرسی کاربران VPN ای که به سرور شما وصل می شوند بسیار مهم است. برای این اعتبار سنجی و برقراری امنیت دو گزینه را می توانید انتخاب نمایید:

۱. اگر در شبکه سرویس دهنده RADIUS داشته باشید، می توانید تنظیم کنید که VPN سرور شما، برای اعتبار سنجی کاربران خود از RADIUS استفاده کند. بدین معنی که اگر یک RADIUS سرور مرکزی در شبکه تان داشته باشید،

اعتبار سنجی تمام کاربران شبکه برای بررسی به این سرور فرستاده تا برای ورود به VPN Server، تایید صلاحیت و یا رد صلاحیت شوند. با این روش کاربران در بین تمام سرورهای VPN به اشتراک گذاشته شده و نیازی به تعریف کاربران در تمامی سرور ها نمی باشد.

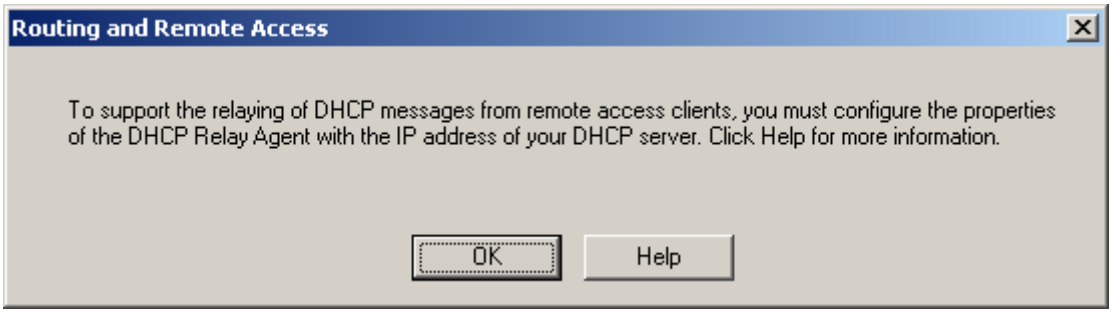
۲. اما گزینه دوم، تمام تقاضاها برای اتصال به VPN Server، از طریق خود سرور و تنظیماتی که در آن نظر گرفته است، مورد بررسی قرار گیرند.

که مطابق شکل زیر، ما اولین گزینه را انتخاب کرده و دکمه Next را می زنیم.

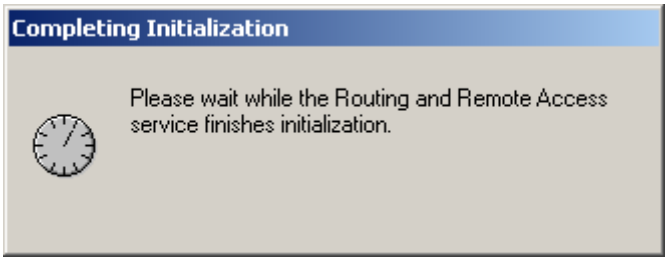


در انتها ممکن است که پنجره ای ظاهر گردد که فقط کافی است دکمه OK را بزنید.

سپس پیامی در مورد پیکربندی DHCP Relay Agent می بینید. روی OK کلیک کنید. در مورد DHCP Relay Agent بعدا بیشتر صحبت خواهیم کرد.



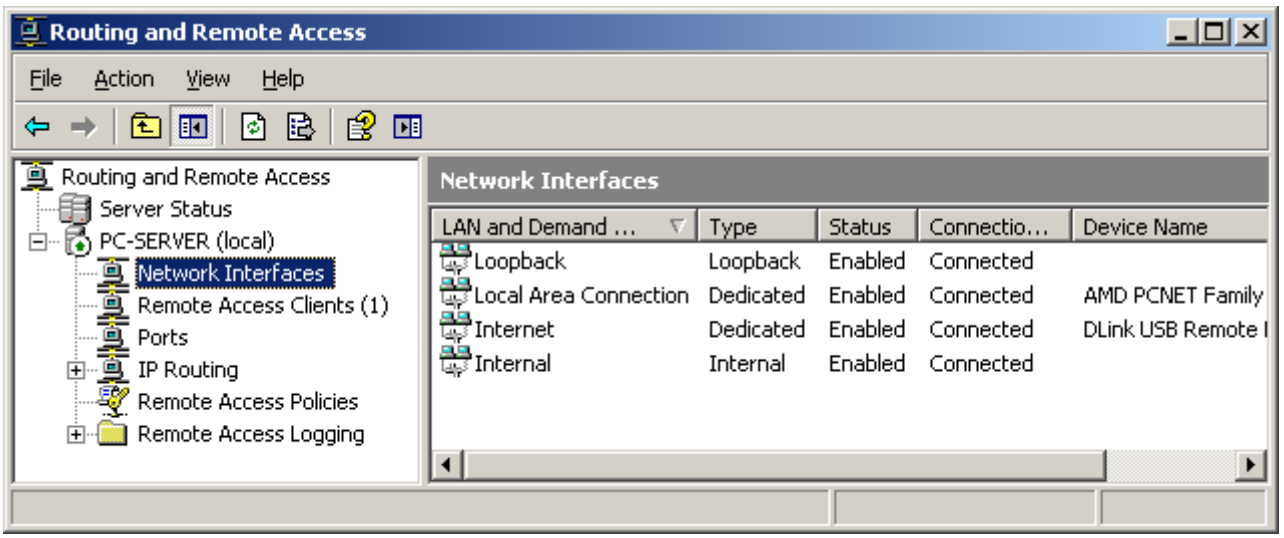
صبر نمایید تا سیستم عملیات نصب را به اتمام برساند. این کار ممکن است تا چند دقیقه به طول بیانجامد.



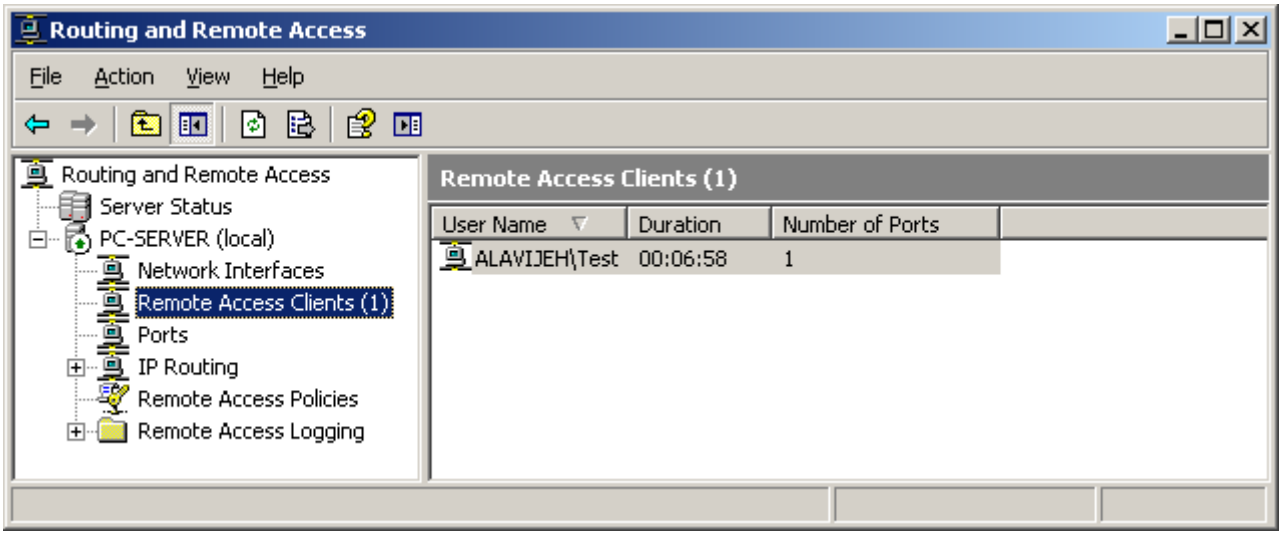
تا این مرحله تنظیمات مربوط به ویزارد نصب RRAS به پایان رسیده و نقش Remote Access / VPN Server به ویندوز ۲۰۰۳ اعطا شده است. اما برای دیدن نتیجه کار پنجره Routing and Remote Access را از مسیر زیر باز کنید.

Start ➔ Administrative Tools ➔ Routing and Remote Access

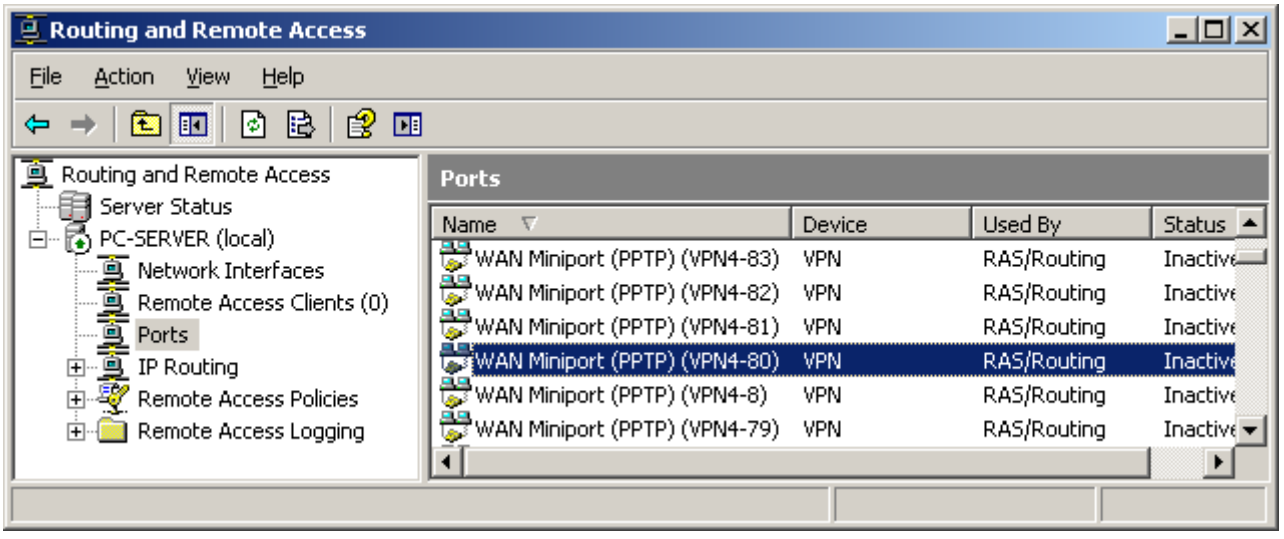
با این کار، صفحه تنظیمات Routing and Remote Access باز می شود؛ که همانطور که از شکل پیداست، این صفحه دارای چندین قسمت می باشد. قسمت Network Interface بیانگر واسط های شبکه ای می باشد که در حال حاضر روی سیستم وجود دارند.



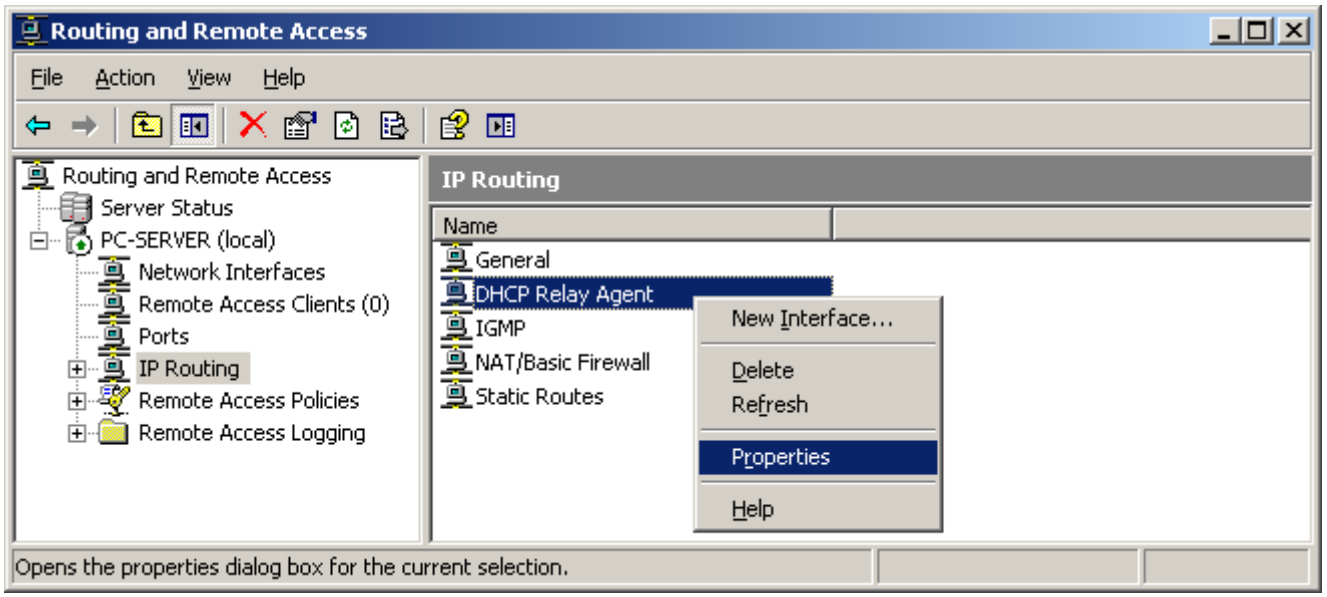
قسمت Remote Access Clients نیز بیانگر کاربرانی می باشد که در حال حاضر از راه دور به سرور (شبکه مجازی) متصل شده اند. از طریق این صفحه می توان ارتباط این کاربران را قطع نمود



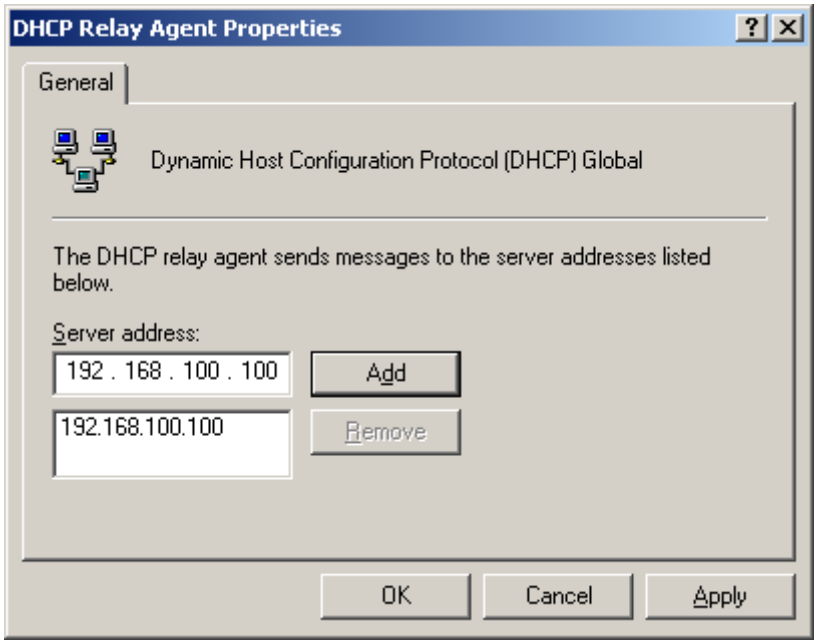
در صفحه بعد می توانید پورت های قابل استفاده توسط VPN Server را مشاهده نمایید.



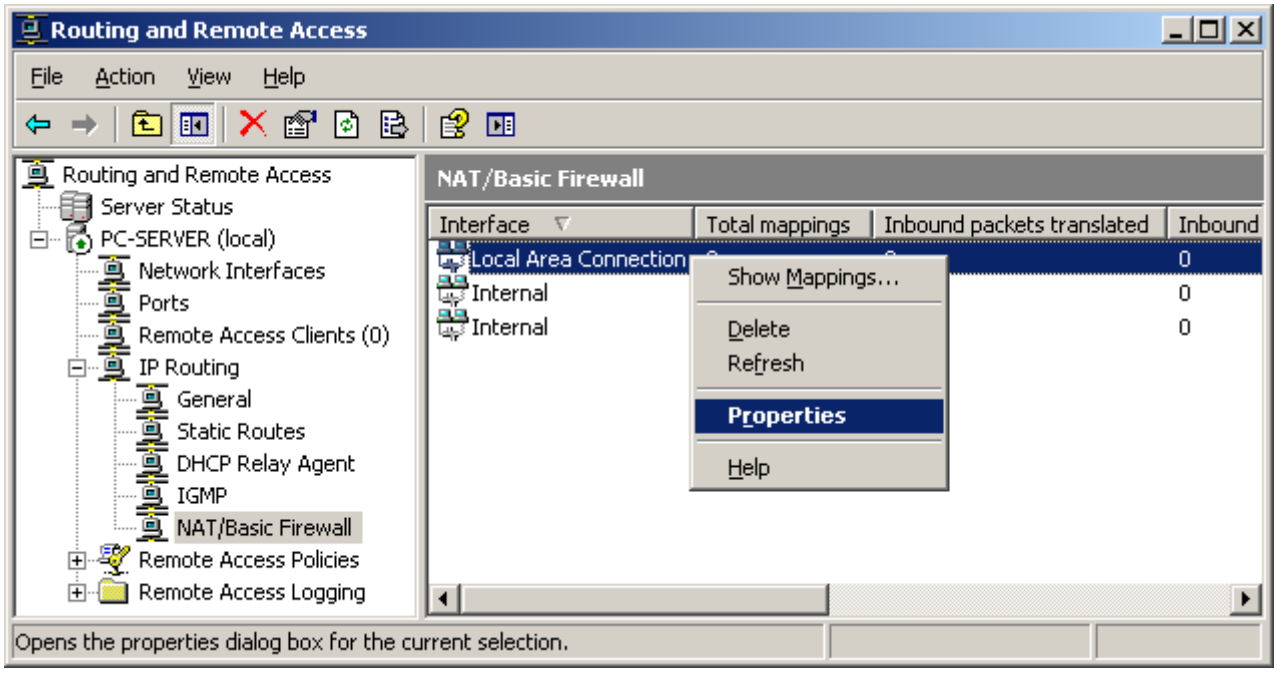
شاید مهمترین قسمت تنظیمات Routing and Remote Access، بخش DHCP Relay Agent باشد. بدین منظور از قسمت IP Routing، روی DHCP Relay Agent راست کلیک نموده و گزینه Properties را انتخاب نمایید.



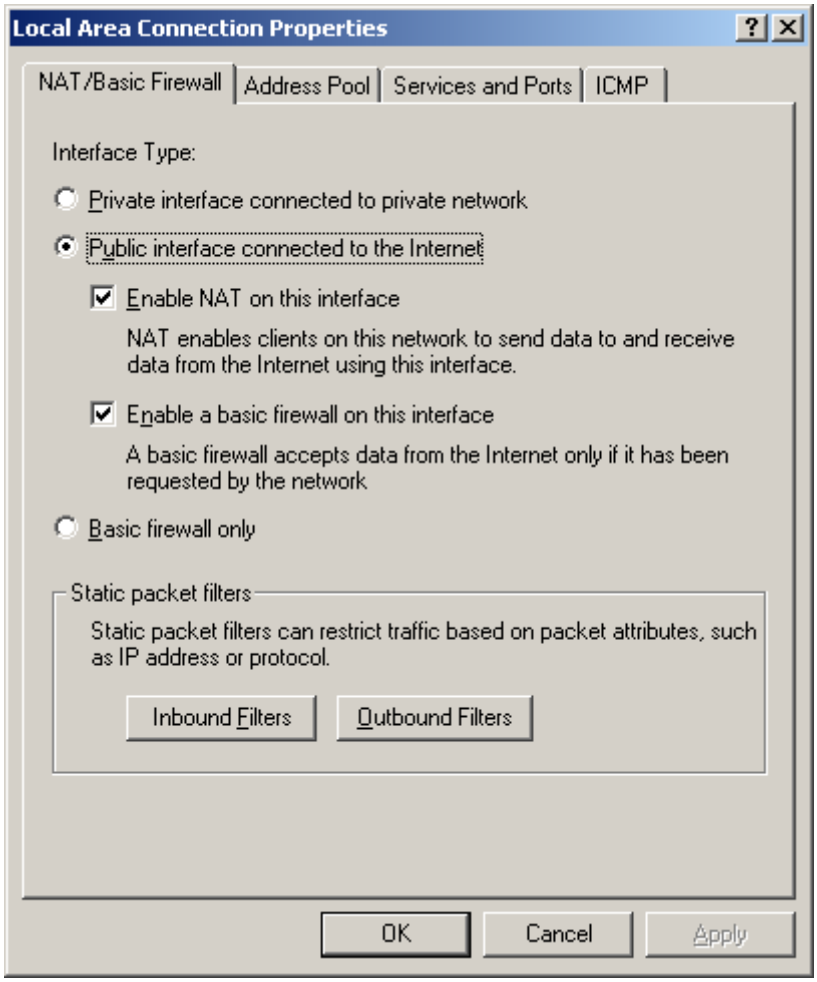
سپس این صفحه، آدرس IP کامپیوتر DHCP Server را به لیست اضافه نمایید. با این کار، سرور شما به عنوان DHCP Relay Agent شناخته می شود و می تواند آدرس IP را با پروتکل DHCP دریافت نماید.



قسمت بعدی که نیاز به معرفی دارد، بخش NAT/Basic Firewall می باشد. از این بخش برای تعیین نقش هر یک از کارت های شبکه و پروتکل های آن، استفاده می شود. بدین منظور در قسمت IP Routing، ابتدا NAT/Basic Firewall را انتخاب نموده و سپس یکی از کارت های شبکه خود را انتخاب نمایید. سپس روی کارت شبکه انتخاب شده، کلیک راست کرده و سپس گزینه Properties را انتخاب نمایید.



سپس در صفحه باز شده، وارد سربرگ NAT/Basic Firewall شود. در این سربرگ، می توان نقش کارت شبکه انتخاب شده را تعیین نمود.



این نقش ها به صورت زیر می باشد:

- **Private Interface connected to private network**: با این گزینه، تعیین می کنید که این کارت شبکه، یک کارت شبکه معمولی (عدم اتصال به اینترنت) می باشد که از آن برای اتصال به شبکه خصوصی استفاده می شود.
- **Public interface connected to internet**: با این گزینه تعیین می کنید که این کارت شبکه، کارت شبکه متصل به اینترنت می باشد؛ یعنی از طریق این کارت می توان به اینترنت دسترسی داشت. انتخاب گزینه Enable NAT on

this device، باعث می شود که این کارت شبکه نقش NAT Server را نیز بازی کند و در نتیجه کاربرانی که به کمک VPN به سرور متصل می شوند، بتوانند به اینترنت نیز دسترسی داشته باشند. انتخاب گزینه Enable a basic firewall on this device نیز باعث می شود که این کارت شبکه، علاوه بر اتصال به اینترنت، نقش دیوار آتشین را نیز بازی کند.

- **Basic firewall only**: از این کارت شبکه، تنها به عنوان یک دیوار آتشین استفاده می شود.

۲۵-۸- تنظیمات کاربران جهت اتصال راه دور به VPN

در ویندوز ۲۰۰۳ بطور پیش فرض، به کاربران اجازه دسترسی به سرور از راه VPN داده نشده است. شما باید به صورت تک به تک، برای هر یک از کاربرانی که می خواهید از راه اینترنت به سرور شما وصل شوند این اجازه را بدهید. برای این کار مراحل زیر را انجام دهید:

اگر در سرور، Domain Controller تعریف کرده باشید (نصب و راه اندازی کامل Domain Controller در فصول پیش، به طور مفصل توضیح داده شده است)، پنجره Active Directory Users and Computers را از مسیر زیر باز کنید.

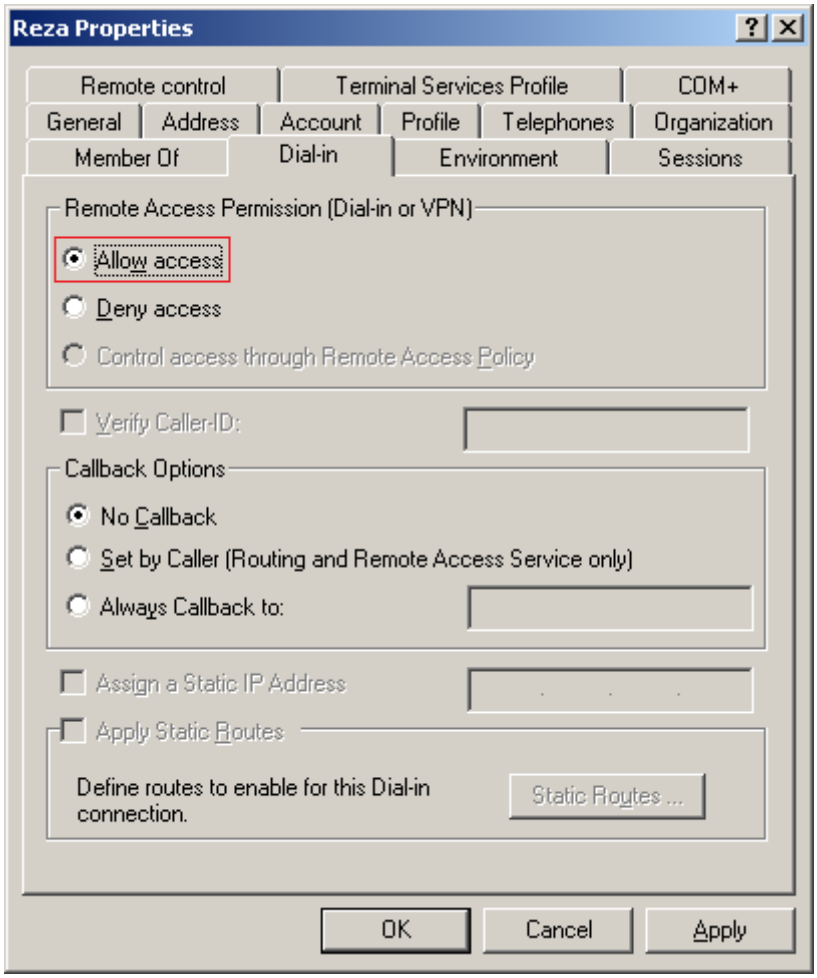
Start ➔ Administrative Tools ➔ Active Directory Users and Computers

در غیر اینصورت و اگر سرور شما در هیچ Domain ای تعریف نشده باشد (و سرور به صورت Standalone باشد)، پنجره Computer Management را از مسیر زیر:

Start ➔ Administrative Tools ➔ Computer Management

باز کنید و صفحه Properties مربوط به کاربری که می خواهید اجازه اتصال به VPN سرور خود را به آن بدهید، را باز کنید و مطابق شکل زیر به قسمت Dial-In بروید و گزینه "Allow access" را انتخاب نمایید.

از طریق این صفحه می توانید تنظیمات امنیتی بیشتری را نیز اعمال نمایید. مثلاً از طریق قسمت Callback Option می توان تنظیم کرد که پس از اتصال Client به سرور، سرور اتصال را قطع نموده و خود را به کامپیوتری خاص متصل نماید؛ اگر کاربر از همان کامپیوتر خاص به سرور متصل شده باشد، قابلیت کار با سرور را پیدا خواهد نمود. یعنی با این کار، کاربر را موظف می کنیم که از کامپیوتری خاص به سرور متصل شود. بدین منظور در قسمت Always Callback To، شما تماس کامپیوتر Client را وارد نمایید. این شماره می تواند شماره تلفن خطی باشد که کاربر به کمک آن به اینترنت متصل شده است.



به خاطر بسپارید که پیاده سازی VPN بار زیادی را روی پردازنده سرور می گذارد و هر چقدر تعداد ارتباطات VPN بیشتر باشد بار زیادتری بر روی سرور خواهد گذاشت. می توانید از یک وسیله سخت افزاری مجزا مانند روتر جهت پیاده سازی VPN کمک بگیرد.

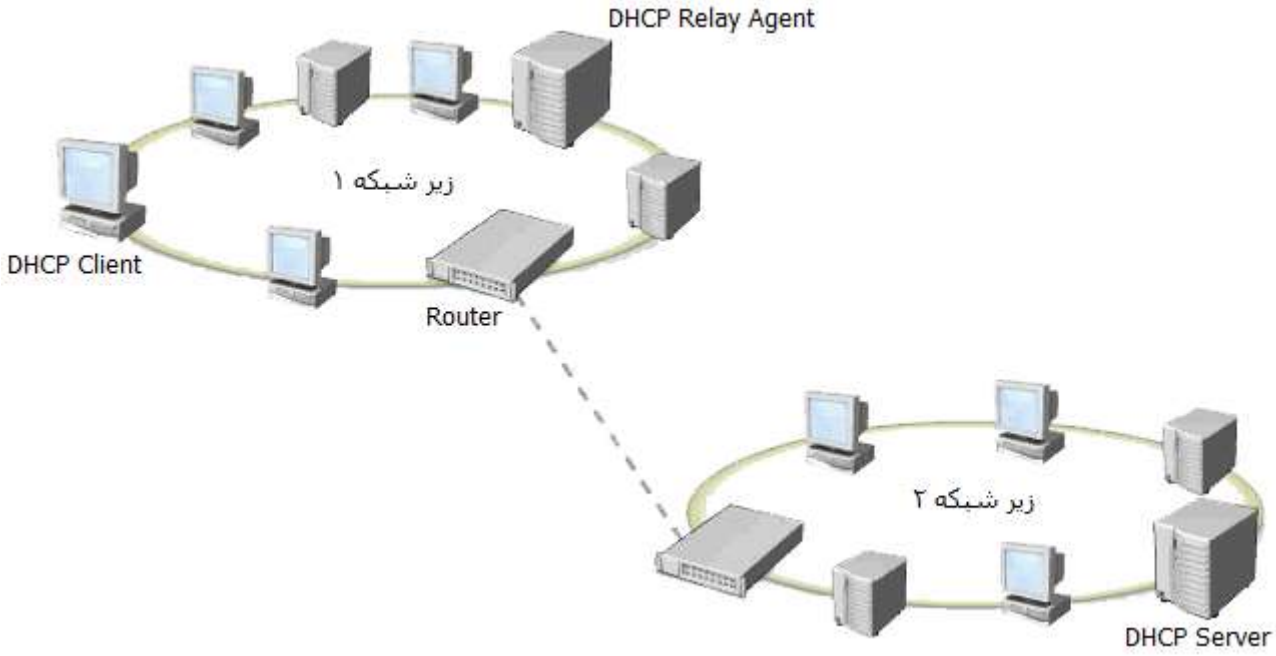
حال برای اتصال به VPN Server، بایستی در دیگر کامپیوتر ها یک اتصال بسازید که نحوه ساخت آن را در همین فصل توضیح داده ایم.

۲۵-۹- معرفی DHCP Relay Agent و نحوه نصب آن

اگر بخواهیم DHCP Relay Agent را مختصرا توضیح دهیم، باید بگوییم که درخواست دریافت آدرس IP توسط Client، به صورت **Broadcast** به تمامی کامپیوتر های شبکه ارسال می شود. در VPN ما با اینترنت سر و کار داریم و در مسیر اینترنت تعداد زیادی روتر وجود دارد. روتر ها، بر عکس سوییچ ها، قابلیت ارسال بسته های Broadcast را ندارند. لذا در VPN Server که از اینترنت استفاده می کند، قابلیت سرویس دهی DHCP Server وجود ندارد. لذا ما از یک DHCP Relay Agent استفاده می کنیم تا کار سرویس دهی DHCP Server را انجام دهد. این سرور بسته های Broadcast را به یک بسته خاص تبدیل نموده و آن را به DHCP Server تحویل می دهد. بعد از به دست آوردن آدرس IP از DHCP Server، آن را به Client تحویل می دهد. Client از جزئیات این کار مطلع نمی شود.

شکل زیر مفهوم DHCP Relay Agent را بهتر نشان می دهد. DHCP Relay Agent زمانی کاربرد دارد که دو زیر شبکه داشته باشیم و این دو زیر شبکه، به کمک مسیر یاب (Router) به یکدیگر متصل شده باشند. مشکل زمانی پیش می آید که یک کامپیوتر موجود در یکی از زیر شبکه ها درخواست آدرس IP کند، اما DHCP Server در زیر شبکه ای دیگر باشد. پیغام درخواست آدرس IP به صورت Broadcast به همه ارسال می شود، اما روتر ها قابلیت عبور بسته های Broadcast را ندارند (مگر اینکه برای این کار پیکربندی شده باشند)؛ لذا درخواست آدرس IP به زیر شبکه دیگر که DHCP Server در آن قرار

دارد ارسال نمی شود. برای حل این مشکل، بایستی از DHCP Relay Agent استفاده نمود. بدین صورت کـه DHCP Relay Agent در زیر شبکه ای قرار می گیرد که Client (درخواست کننده) در آن قرار دارد. به هنگـام درخواسـت آدرس IP توسـط Client و به صورت Broadcast، چون DHCP Relay Agent آدرس DHCP Server را دارد، DHCP Relay Agent این پیـام را به صورت Unicast به روتر می دهد و روتر نیز آن را به DHCP Server می دهـد. DHCP Relay Agent پـس از دریافـت پاسخ از DHCP Server، آدرس دریافت شده را به Client تحویل می دهد.



در ادامه به چگونگی پیاده سازی DHCP Relay Agent می پردازیم.

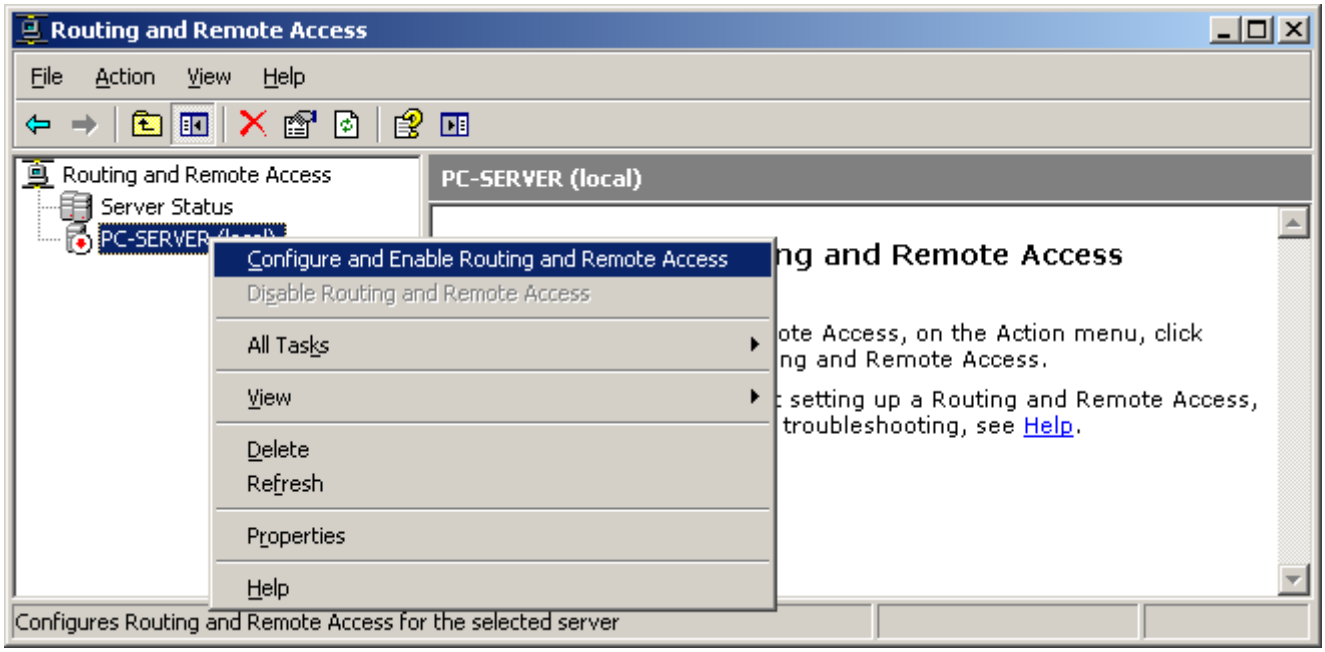
برای پیاده سازی DHCP Relay Agent، دو راه داریم:

۱. از روتر های فیزیکی و سخت افزاری استفاده کرده و گزینه ی Relay DHCP Packets را روی آن فعال می کنیم.
۲. از Windows Server 2003 به عنوان روتر نرم افزاری استفاده می نماییم.

ما در اینجا گزینه دوم را انتخاب خواهیم کرد. بدین منظور در ویندوز سرور برنامه Routing and Remote Access را از مسیر زیر باز کنید.

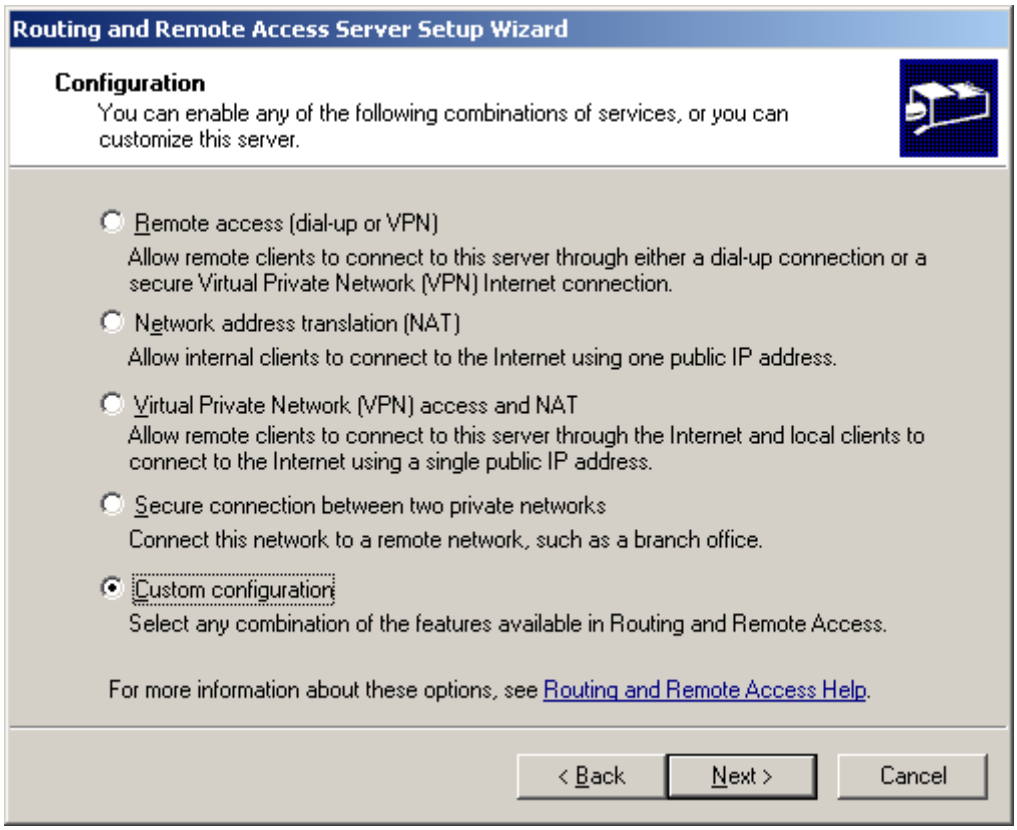
Start ➔ Administrative Tools ➔ Routing and Remote Access

در صفحه باز شده، بر روی سـرور، راسـت کلیـک نمـوده و گزینـه Configure and Enable Routing & Remote Access را انتخاب نمایید. توجه نمایید که سرور بایستی غیر فعال باشد. اگر سرور فعال بود، در منوی باز شده، گزینه Disable Routing and Remote Access را انتخاب نمایید.

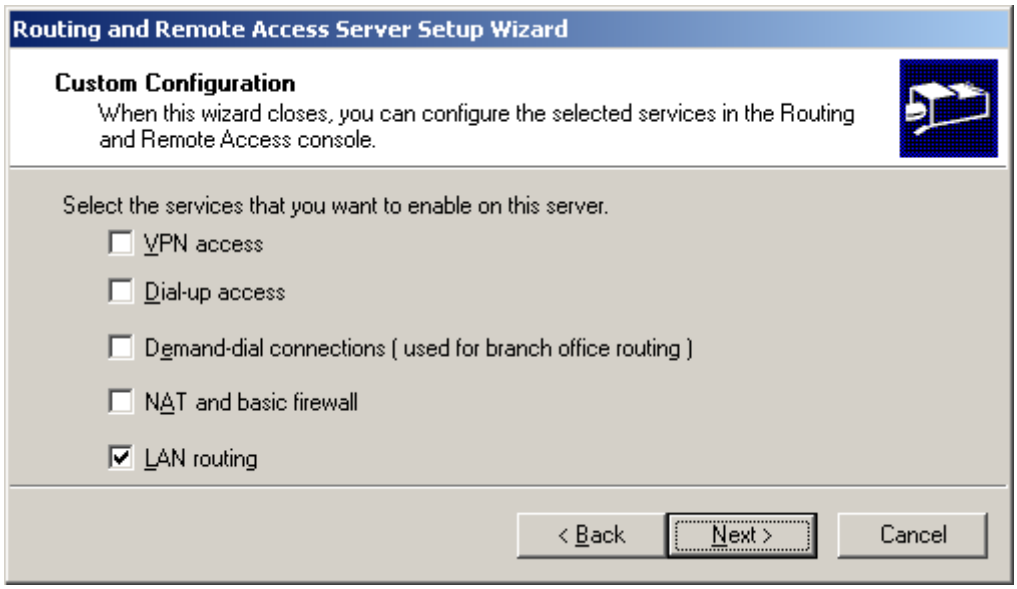


صفحه باز شده، به غیر از راهی برای پیاده سازی DHCP Relay Agent، شامل راه هایی برای تبدیل کامپیوتر به یک RAS Server (که می تواند VPN و یا Dial-Up Based باشد) و غیره (مثل پیاده سازی NAT) هم می باشد که فعلا مربوط به بحث ما نمی شود.

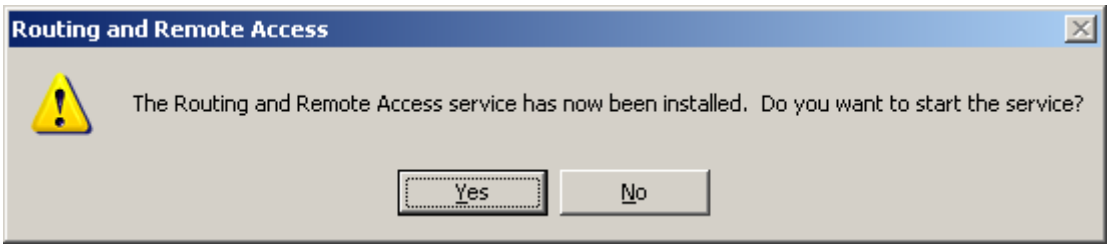
در صفحه باز شده، گزینه Custom Configuration را انتخاب نموده و روی Next کلیک کنید:



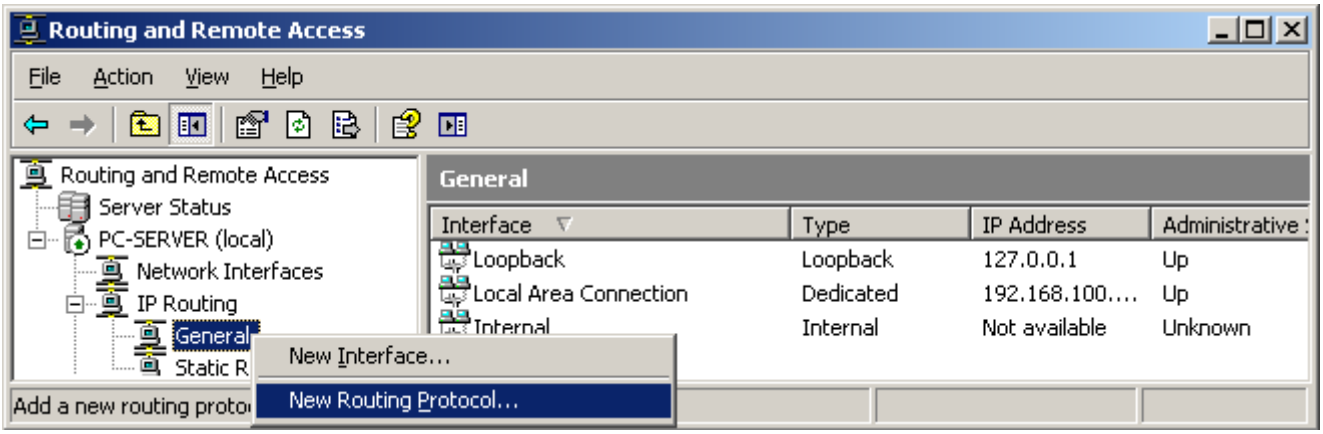
حالا ما می توانیم این کامپیوتر را به صورت دستی تبدیل به روتر کنیم. در اینجا ما می خواهیم که این کامپیوتر فقط بتواند بسته های Subnet های مختلف رو به مقصدشان هدایت کند و به همین دلیل گزینه ی LAN Routing رو انتخاب کرده و روی Next کلیک نمایید.



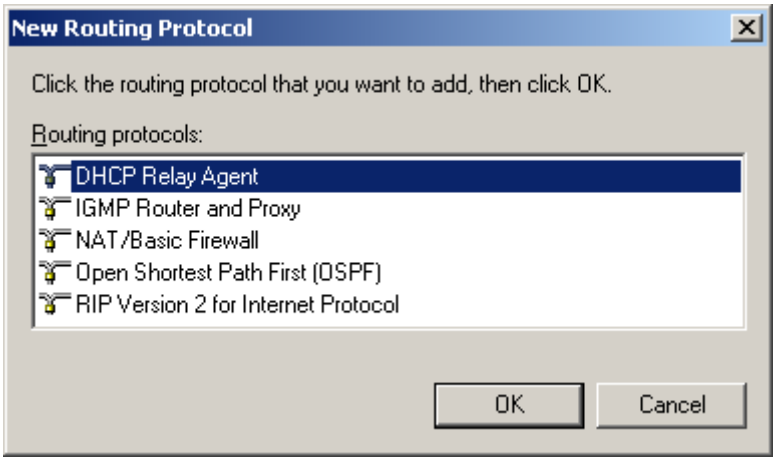
تا اینجا کار نصب تمام می شود. سیستم از شما سوال می پرسد که آیا سرویس Routing and Remote Access فعال شود یا خیر؟ گزینه Yes را انتخاب نمایید.



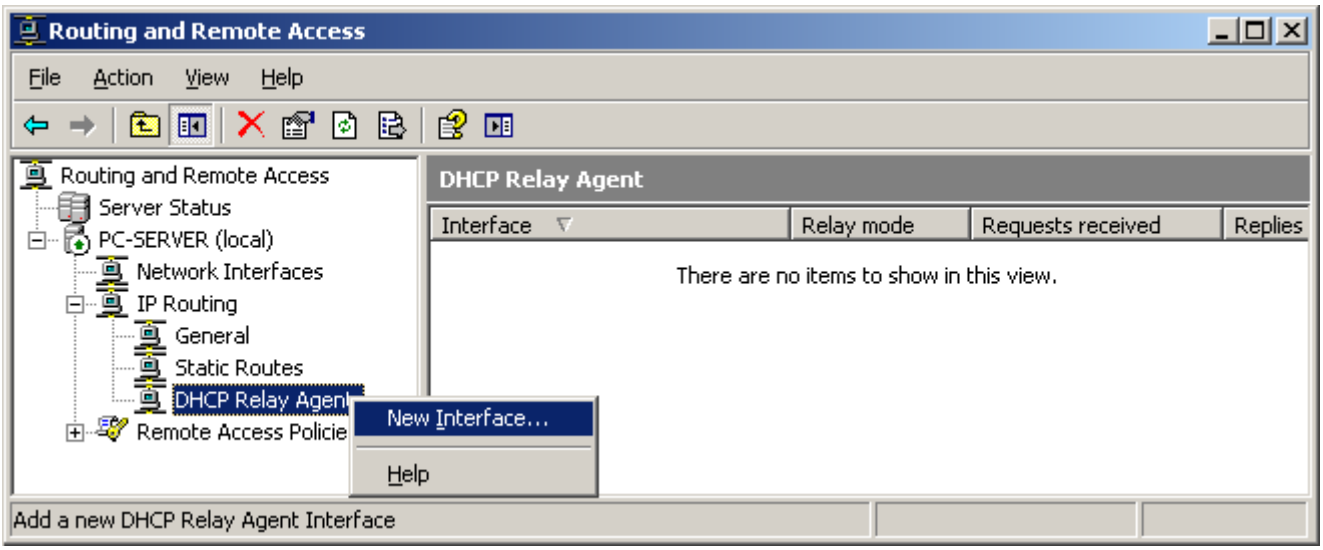
مجددا به صفحه اصلی باز می گردیم. در اینجا ما می خواهیم که یک پروتکل مسیر یابی جدید به پروتکلهای فعلی سیستم اضافه کنیم تا بتواند بسته های درخواست DHCP رو هدایت کند. لذا از قسمت IP Routing، روی گزینه General راست کلیک نموده و گزینه New Routing Protocol را انتخاب نمایید.



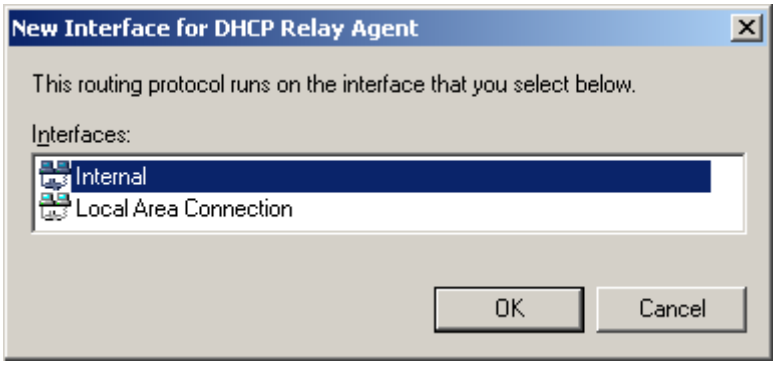
در صفحه باز شده، گزینه DHCP Relay Agent را انتخاب نمایید تا این سرویس روی سیستم شما نصب شود. سپس روی OK کلیک کنید.



وقتی که به صفحه اصلی برگردید، متوجه می شوید که در زیر مجموعه های IP Routing، یک قسمت جدید بـه نـام DHCP Relay Agent اضافه شده است. حالا روی آن راست کلیک کرده و گزینه ی New Interface رو انتخاب نمایید. در اینجـا مـی خواهیم به این سیستم بگوییم که پاکت های اطلاعاتی که از کدام کارت شبکه دریافت می کند را Relay کند.



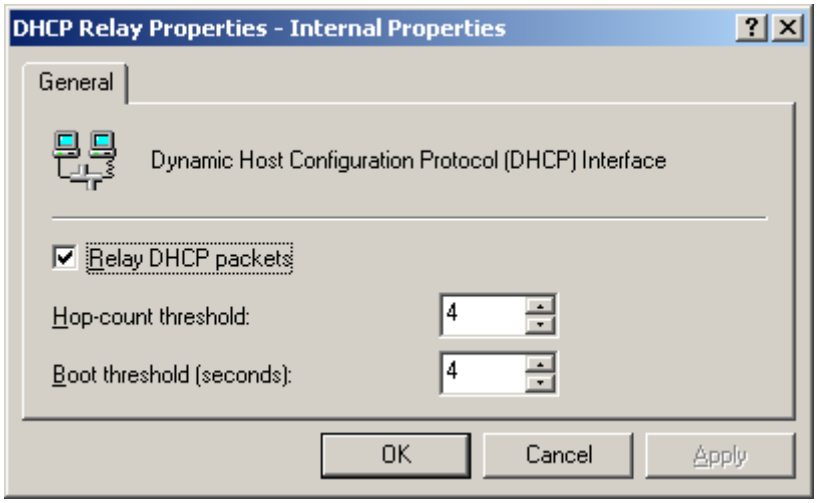
حالا باید کارت شبکه ای که Subnet های مختلف به آن وصل می شوند را انتخاب کنید. این کارت شبکه، همان کارت شـبکه ای است که کامپیوتر دروازه (Gateway) Subnetها چه با Switch و چه با Hub به آن وصل می شوند. پـس یـک دفعـه یـک کارت شبکه ای که اصلا به جایی وصل نیست را انتخاب نکنید! مثلاً در این تصویر من دو تا کارت شبکه دارم که کارت شـبکه با نام Internal را انتخاب کرده ام.



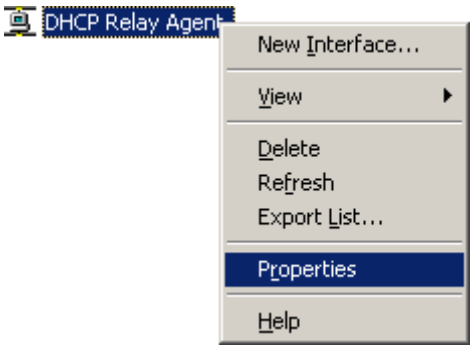
سپس صفحه زیر باز می شود. در این صفحه، سه گزینه می بینید. گزینه Relay DHCP Packet به معنای فعال بودن سرویس Relay است. آن را انتخاب نمایید.

گزینه Hop-Count Threshold، معین می کند که Relay Agent باید بسته ها را تا چند تا روتر مسیر دهی کند و اگر مثلاً از ۴ تا بیشتر بشود، مسیر دهی و ارسال درخواست آدرس IP را دیگر ادامه نمی دهد. گزینه بعدی هم Boot Threshold نام دارد که تعداد ثانیه هایی است که Relay Agent، با در نظر گرفتن احتمال اینکه ممکن است یک DHCP Server درون زیر شبکه

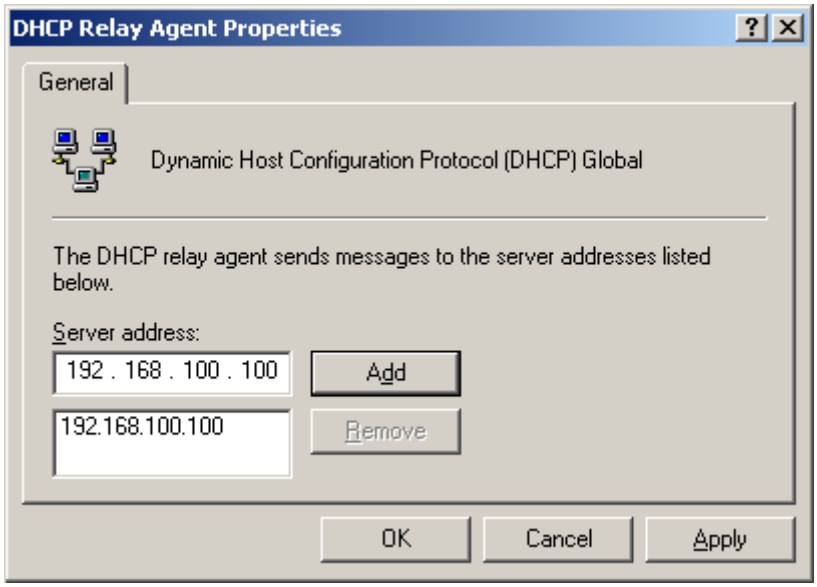
بوده باشد، صبر کرده و پیام درخواست IP را نمی فرستد. اگر این ثانیه ها تمام شود، Relay Agent، اقدام به فرستادن پیام می کند.



تا اینجا کار تنظیمات ما انجام شد. تنها کاری که باقی می ماند، این است که به DHCP Relay Agent بگوییم که DHCP Server در کدام زیر شبکه (Subnet) قرار دارد. لذا روی گزینه DHCP Relay Agent راست کلیک نموده و گزینه Properties را انتخاب نمایید.



در صفحه باز شده، آدرس سروری که سرویس DHCP روی آن نصب است را اضافه نمایید.



توجه: ممکن است تا اینجا سر در گم شده باشید که چرا این تنظیمات را روی سرور انجام دادیم؟ جواب این است که ما این کار ها را روی سرور اصلی انجام ندادیم، بلکه این تنظیمات را روی کامپیوتری انجام دادیم که نقش DHCP Relay Agent را بازی می کند و این نقش فقط در ویندوز سرور وجود دارد. کامپیوتری که نقش DHCP Relay Agent را بازی می

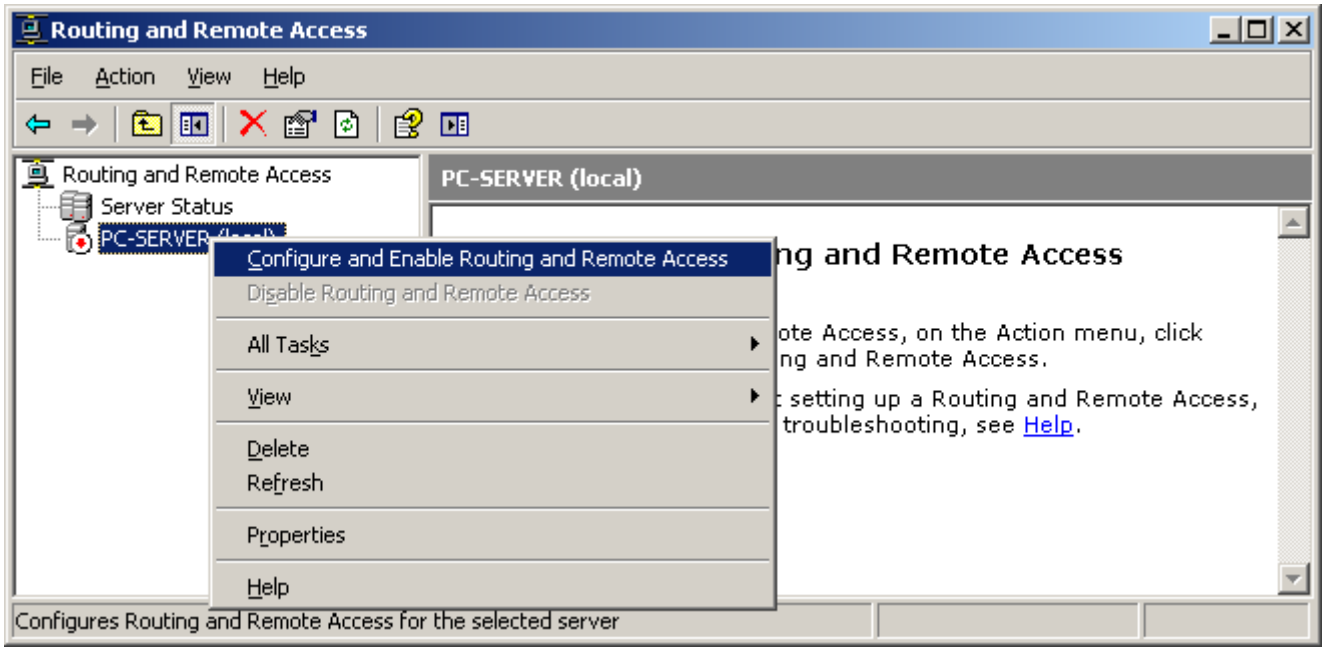
کند، متفاوت از سرور اصلی و DHCP Server می باشد. یعنی بایستی در یک زیر شبکه که DHCP Server ندارد، یک کامپیوتر مجزا که روی آن ویندوز سرور نصب است را قرار داده و نقش DHCP Relay Agent را به آن بدهیم.

۲۵-۱۰- نصب VPN Server با داشتن یک کارت شبکه

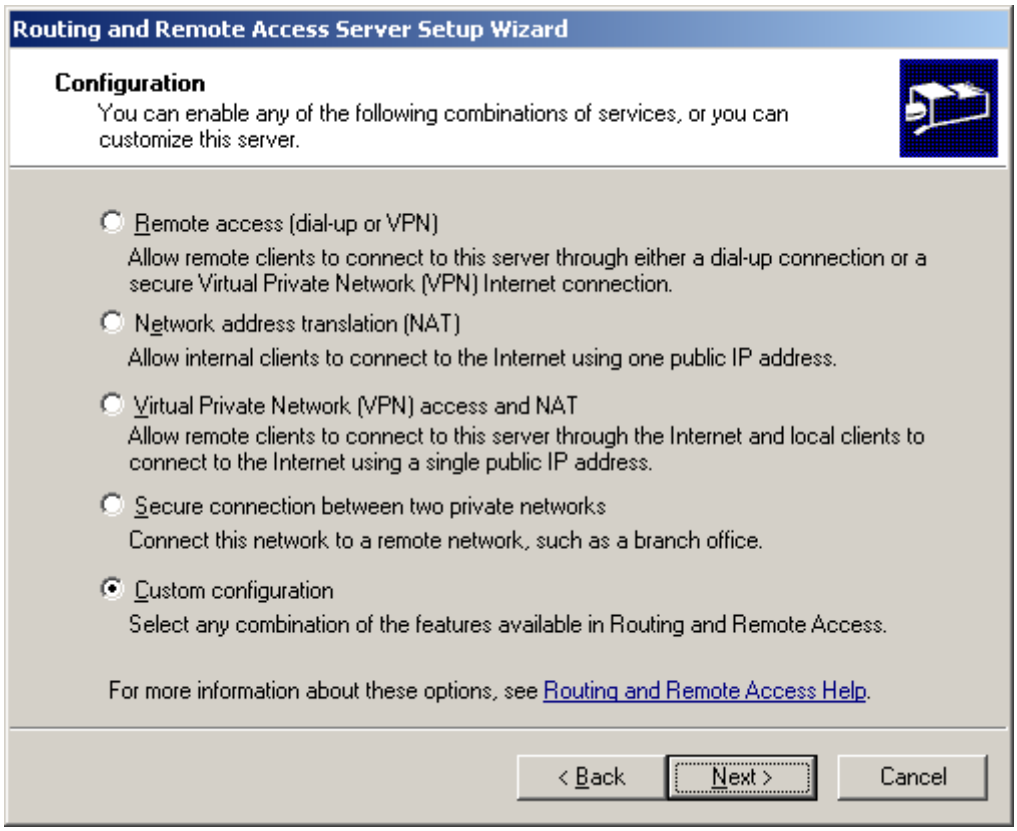
در قسمت قبلی، نحوه نصب VPN Server روی ویندوز سرور ۲۰۰۳ را آموزش دادیم. در ابتدای بحث گفتیم که برای نصب VPN Server، بایستی حداقل دو کارت شبکه داشته باشیم؛ یکی برای اتصال به اینترنت و دیگری برای سرویس دهی به کاربران راه دور. اما اگر یک کارت شبکه بیشتر نداشتیم و بخواهیم از همین تک کارت شبکه، هم برای اتصال به اینترنت و هم برای سرویس دهی به کاربران استفاده کنیم چطور؟ آیا راه حلی وجود دارد؟ جواب مثبت است. بدین منظور، بایستی سرور را دستی پیکربندی نماییم. برای این کار، ابتدا سرویس Windows Firewall/Internet Connection Sharing (ICS) را غیر فعال نمایید که آن را در بخش قبل توضیح دادیم. سپس پنجره Routing and Remote Access را از مسیر زیر باز کنید.

Start ➔ Administrative Tools ➔ Routing and Remote Access

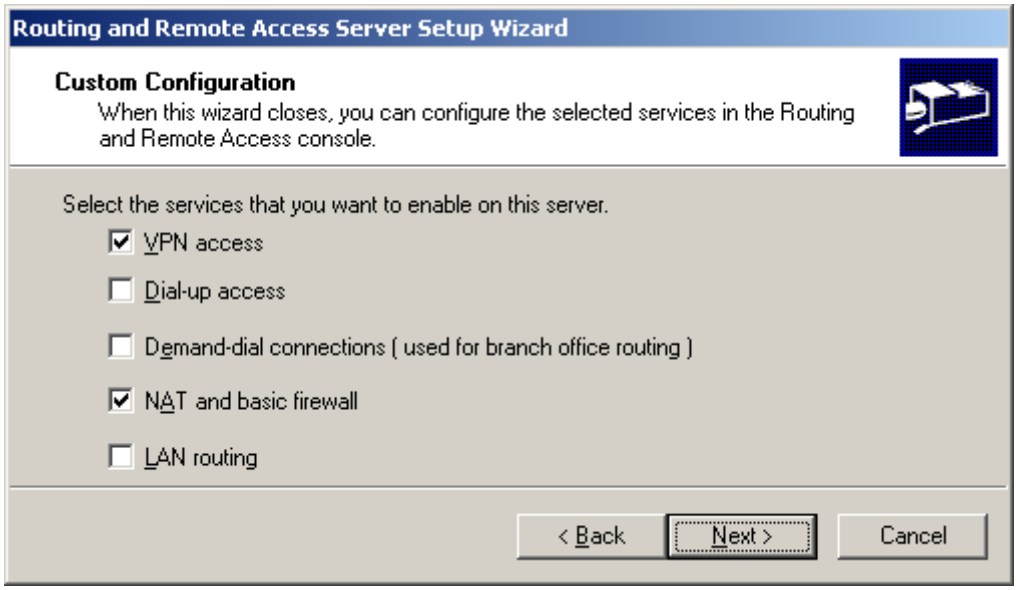
با این کار، صفحه تنظیمات Routing and Remote Access نمایان می شود. برای شروع کار و نصب VPN Server روی ویندوز سرور با یک کارت شبکه، روی نام سرور راست کلیک نموده و گزینه Configure and Enable Routing and Remote Access را انتخاب نمایید.



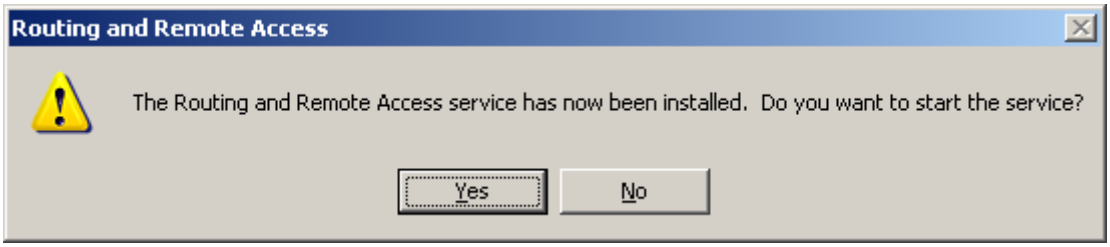
در صفحه باز شده، گزینه Custom Configuration را انتخاب نموده و روی Next کلیک کنید.



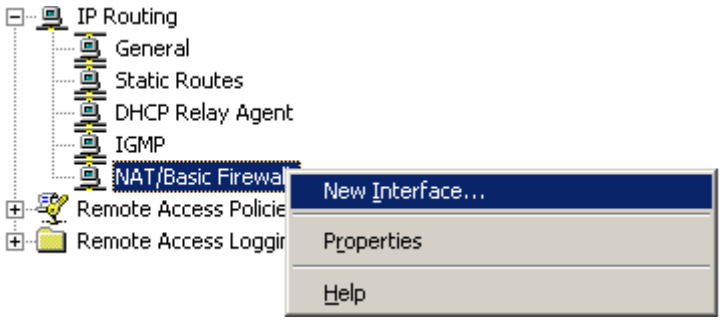
در صفحه بعدی، دو گزینه VPN Access و NAT and Basic Firewall را انتخاب نمایید تا هر دو سرویس روی سیستم شما نصب شود. سپس Next را بزنید. در نهایت نیز روی Finish کلیک کنید تا عملیات نصب به پایان برسد.



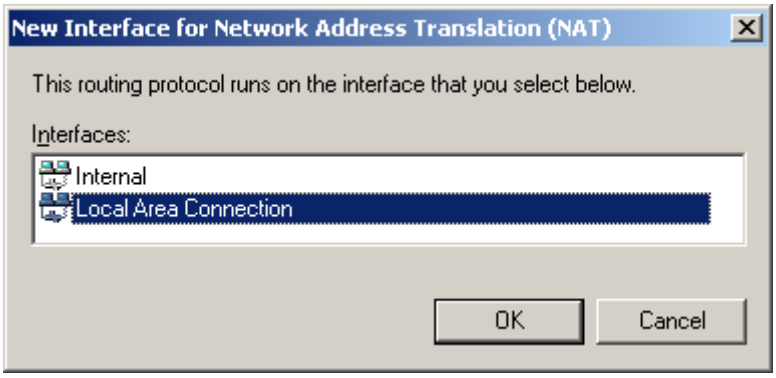
تا اینجا کار نصب تمام می شود. سیستم از شما سوال می پرسد که آیا سرویس Routing and Remote Access فعال شود یا خیر؟ گزینه Yes را انتخاب نمایید.



مجددا به صفحه اصلی باز می گردیم. پس از راه اندازی سرویس، از قسمت IP Routing، روی گزینه NAT/Basic Firewall راست کلیک نموده و گزینه New Interface را انتخاب کنید تا یک کارت شبکه را برای سرویس دهی انتخاب نمایید.



در صفحه باز شده، کارت شبکه ای که قرار است VPN روی آن اعمال شود را انتخاب نمایید. می خواهیم تنظیمات Firewall این کارت شبکه را تغییر دهیم.

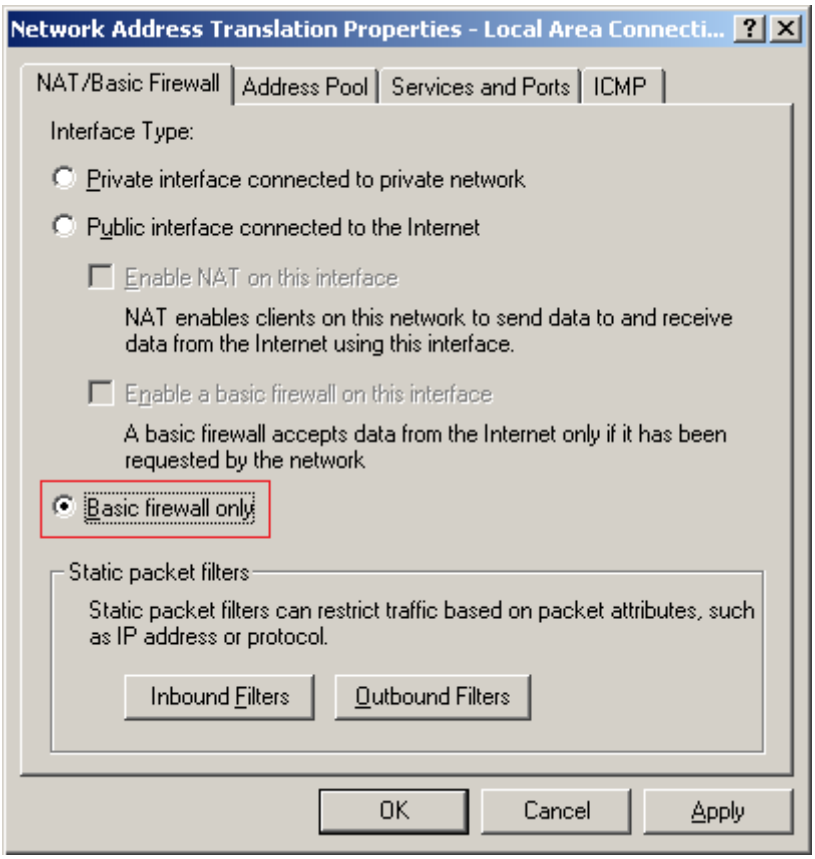


با کلیک روی دکمه OK، صفحه تنظیمات زیر باز می شود. در سربرگ NAT/Basic Firewall، گزینه Basic firewall only را انتخاب نمایید تا سرور به عنوان یک Firewall ساده عمل کند.

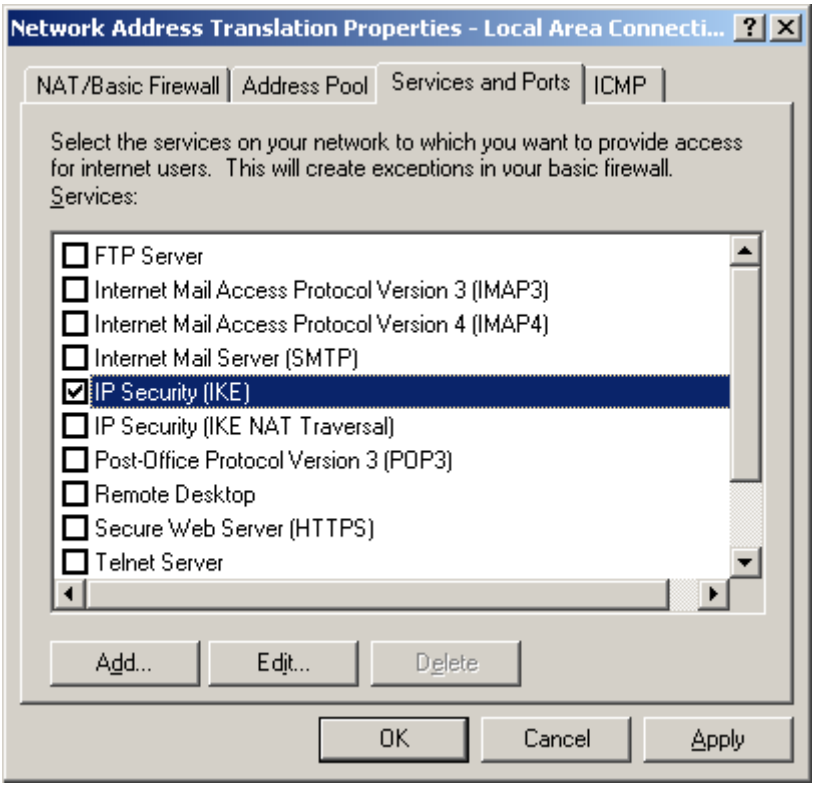
در شکل زیر، گزینه Private interface connected to private network، می گوید که این کارت شبکه، یک کابل شبکه می باشد که برای اتصال به شبکه خصوصی از آن استفاده می شود.

گزینه Public interface connected to the internet، بیان می کند که از این کارت شبکه برای اتصال به اینترنت استفاده می شود. اگر این گزینه را انتخاب نموده و سپس گزینه Enable NAT on this interface را انتخاب نمایید، کاربرانی که با VPN، به این سرور متصل می شوند، قابلیت دسترسی به اینترنت را نیز خواهند داشت. گزینه Enable a basic firewall on this interface نیز باعث می شود که این کارت شبکه، علاوه بر اتصال به اینترنت، نقش دیوار آتشین را نیز داشته باشد.

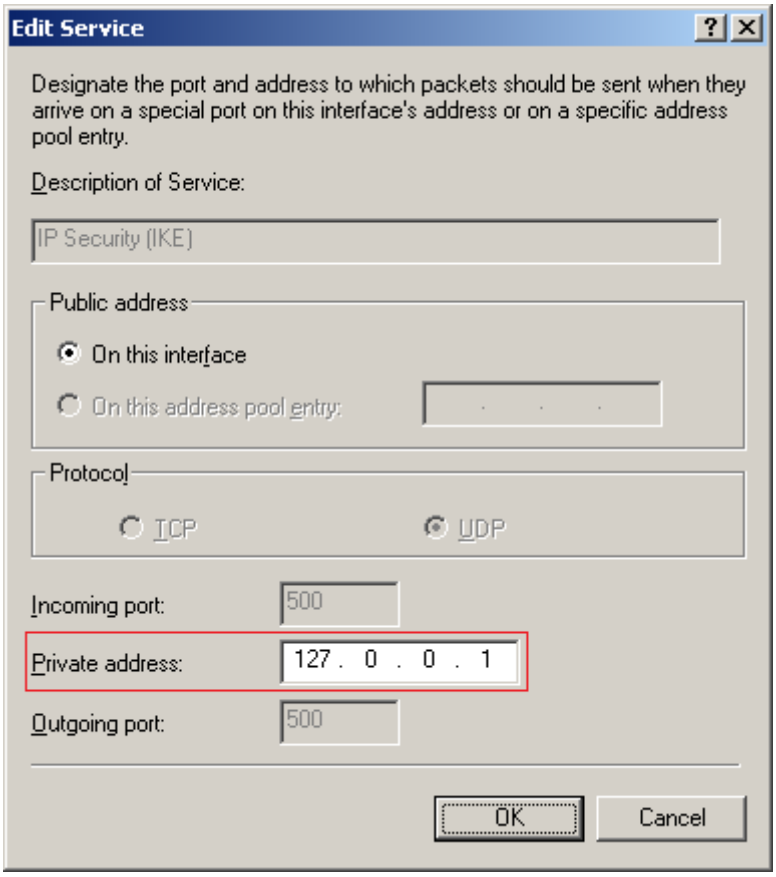
گزینه Basic firewall only نیز، تنها نقش یک دیوار آتشین را به این کارت شبکه می دهد.



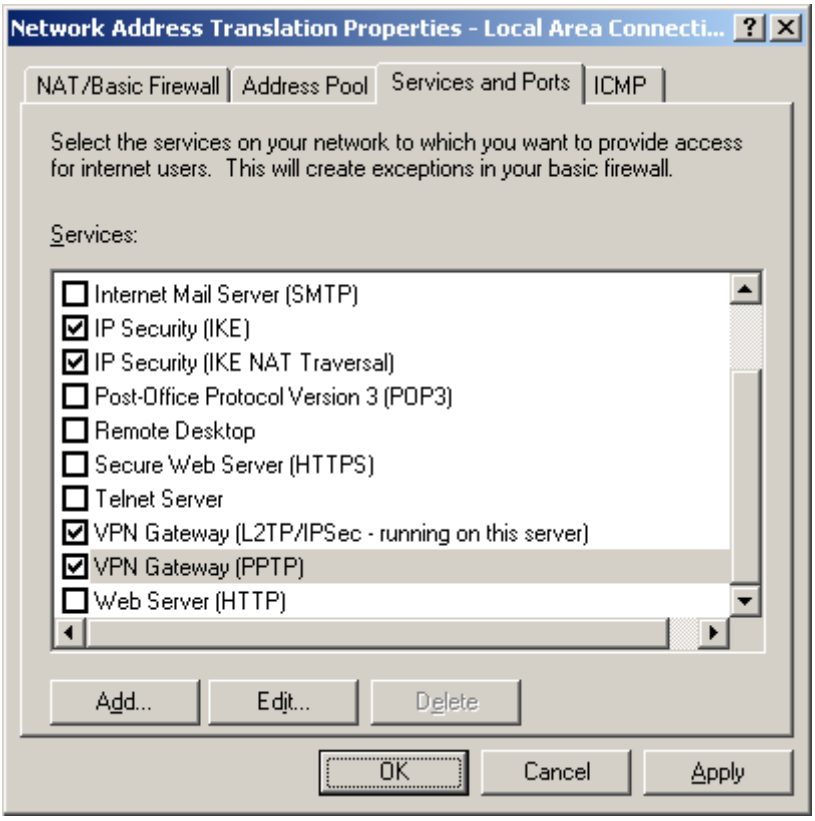
سپس وارد سربرگ Services and Ports شوید. ابتدا گزینه IP Security (IKE) را انتخاب نمایید.



به محض انتخاب این گزینه، صفحه زیر باز می شود. در این صفحه بایستی تنظیم نمایید کـه NAT پـس از دریافـت ترافیـک (اطلاعات) از Firewall، آن ها را بایستی به کجا مسیر دهی کند؟ شما تنظیم نمایید که این ترافیـک هـا را بـه سـرور محلـی مسیر دهی کند. لذا در قسمت آدرس IP، آدرس محل خود، یعنی 127.0.0.1 را وارد نمایید. صفحه زیر، به ازاء انتخاب گزینـه های دیگر نیز باز می شود. برای آن ها نیز همین آدرس IP را وارد نمایید.

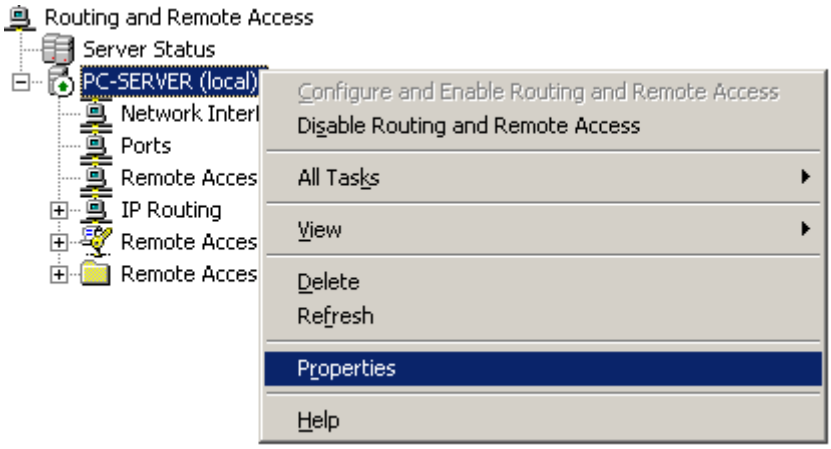


پـس از تاییـد، گزینـه هـای IP Security (IKE NAT Traversal)، VPN Gateway (L2TP/IPSec) و VPN Gateway (PPTP)را انتخاب نمایید. آدرس 127.0.0.1 را نیز برای آن ها ثبت نمایید.

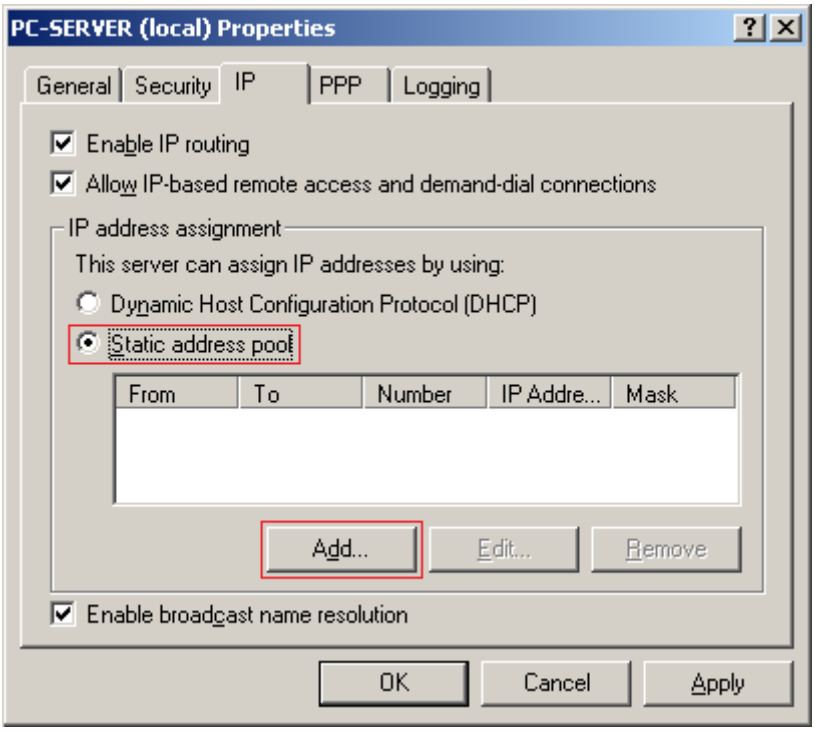


حال نوبت به تنظیم محدوده آدرس IP می شود.

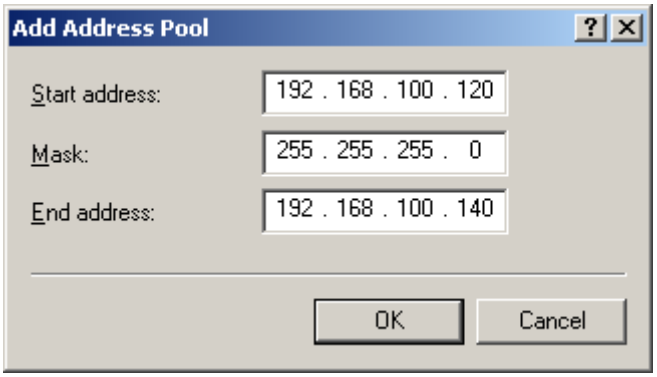
روی نام سرور راست کلیک نموده و Properties را انتخاب نمایید.



سپس وارد سربرگ IP شوید. در اینجا می خواهیم محدوده آدرس قابل تخصیص به Clientها را تعیین نماییم. لذا ابتدا گزینه Static address pool را انتخاب نمایید. سپس برای افزودن محدوده جدید، روی Add کلیک نمایید.

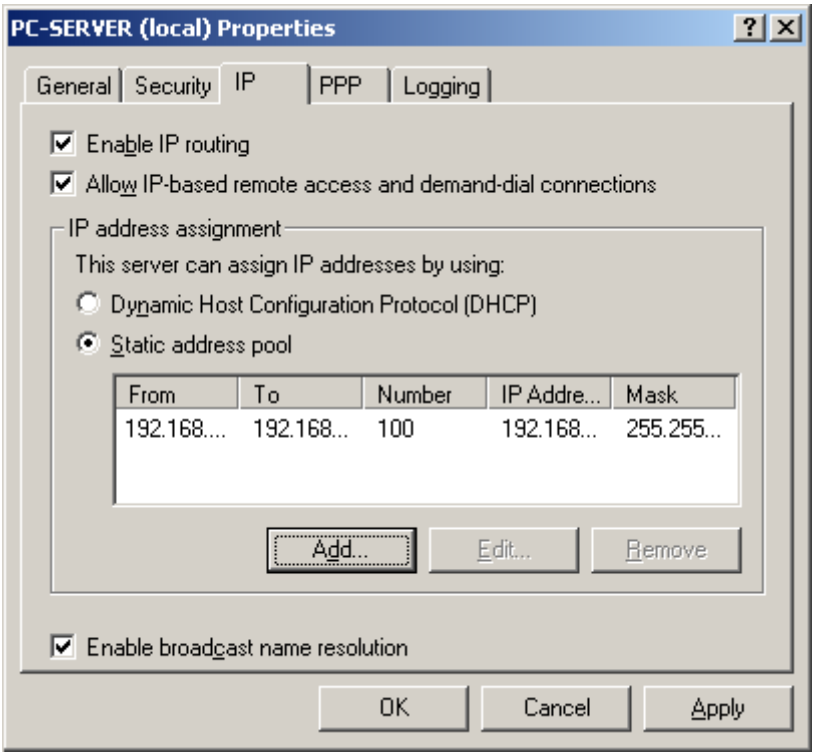


در صفحه باز شده، محدوده جدید را وارد نمایید. در این شکل ابتدا آدرس شروع، سپس Subnet Mask شبکه و سپس آدرس پایان را وارد نمایید. این تصویر با تصویری که قبلاً در مورد محدوده آدرس IP مشاهده نمودید، اندکی متفاوت است.



نکته مهم: دقت فرمایید که محدوده آدرس وارد شده، تداخلی با آدرس کامپیوتر هایی که اکنون به صورت محلی با کامپیوتر سرور شبکه هستند، نداشته باشد.

با این کار، محدوده آدرس وارد شده، به محدوده آدرس های موجود اضافه می شود. در نهایت روی دکمه OK کلیک نمایید.



تا اینجا، VPN Server ما، به درستی نصب شده است. فقط تنظیمات کاربران می ماند که مشخص نماییم که کدام کاربر، حق دسترسی به شبکه VPN را از راه دور دارد؟ که بایستی وارد قسمت Active Directory Users & Groups شویم.

نحوه تنظیمات کاربران برای اتصال به VPN را در همین فصل توضیح داده ایم.

فصل ۲۶

Mail Server

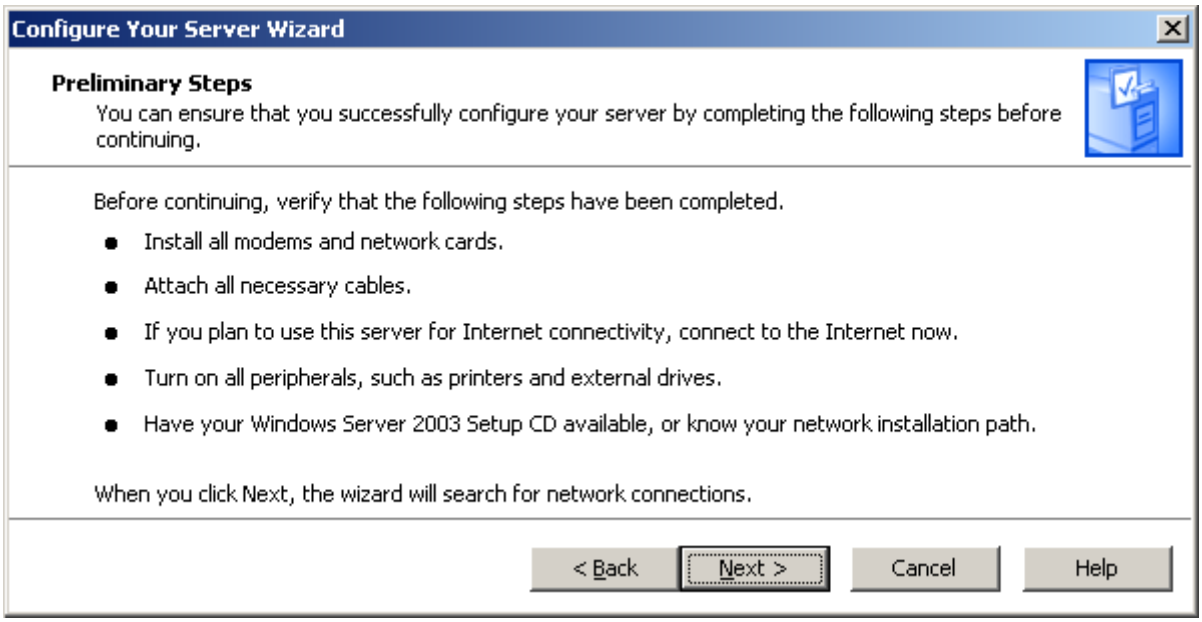
۲۶-۱- نصب Mail Server

Mail Server، این امکان را به ما می دهد که برای کاربران شبکه خود ایمیل بسازیم و محل و آدرس این ایمیل ها، سرور خودمان باشد.

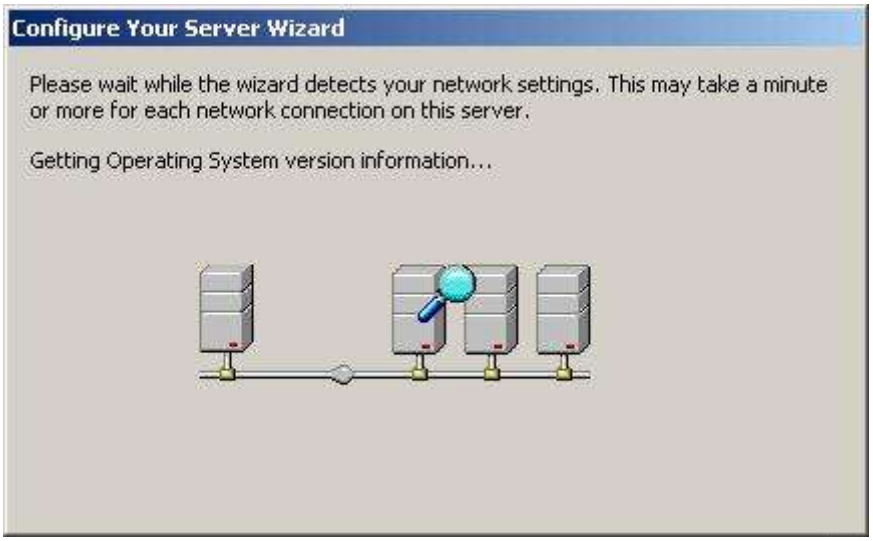
برای نصب Mail Server بر روی ویندوز سرور ۲۰۰۳، مسیر زیر را اجرا کنید: Start ➔ Administrative Tools ➔ Configure Your Server Wizard این بخش جهت افزودن نقش (Role) به سرور مورد استفاده قرار می گیرد.

ابتدا صفحه خوش آمد گویی باز می شود. در این صفحه، دکمه Next را بزنید.

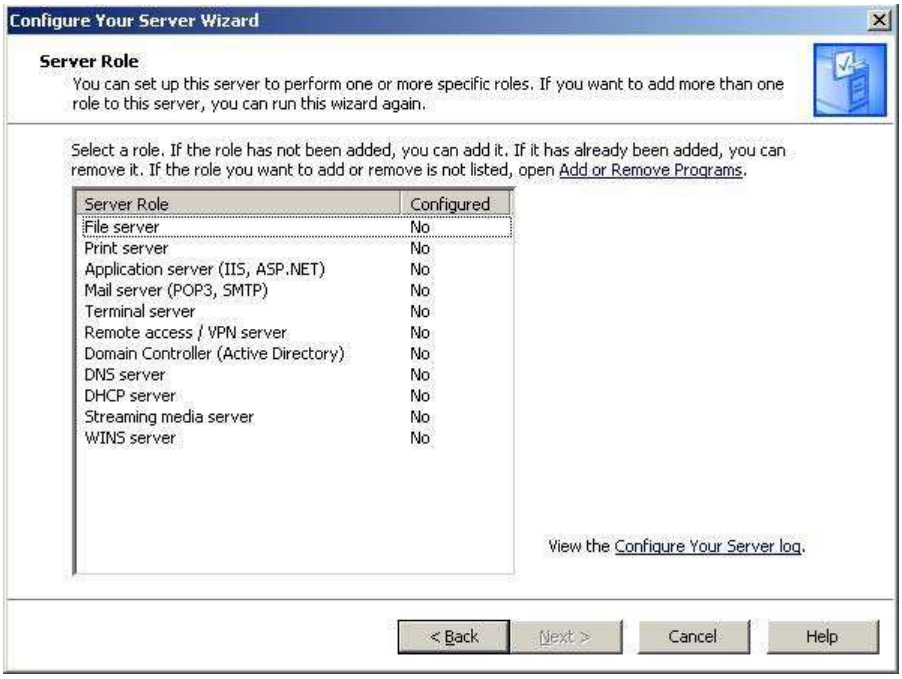
با این کار صفحه زیر ظاهر می شود که باید بر روی دکمه Next کلیک کنید.



پس از کلیک بر روی Next، صفحه زیر ظاهر می شود:

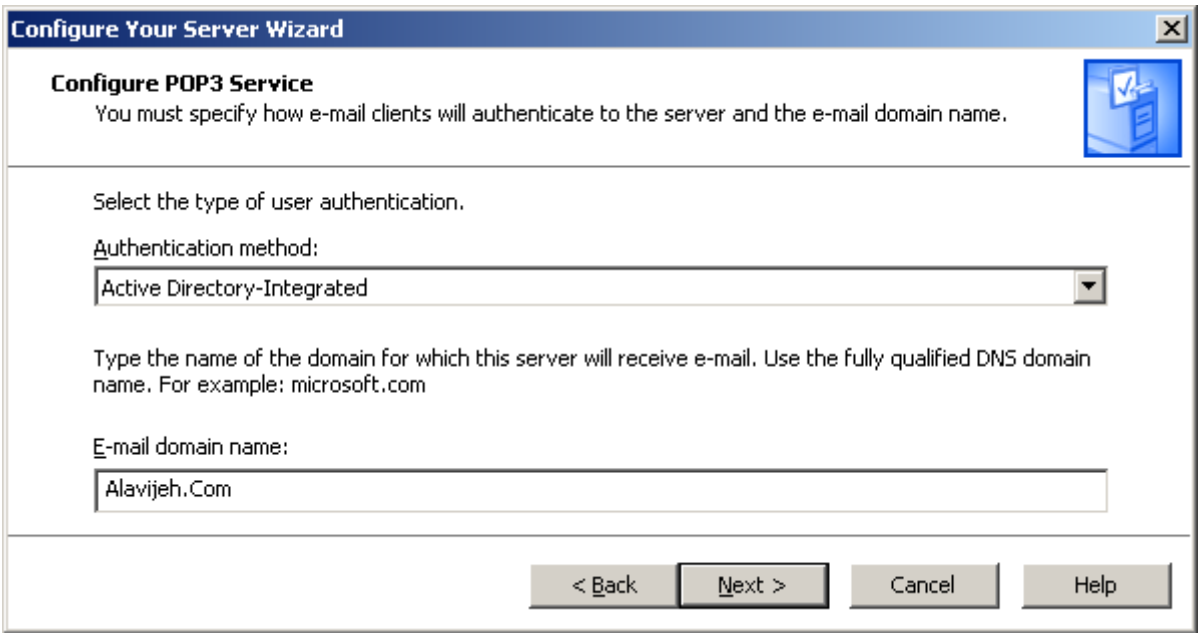


و سپس به صورت اتوماتیک صفحه زیر نمایان خواهد شد:

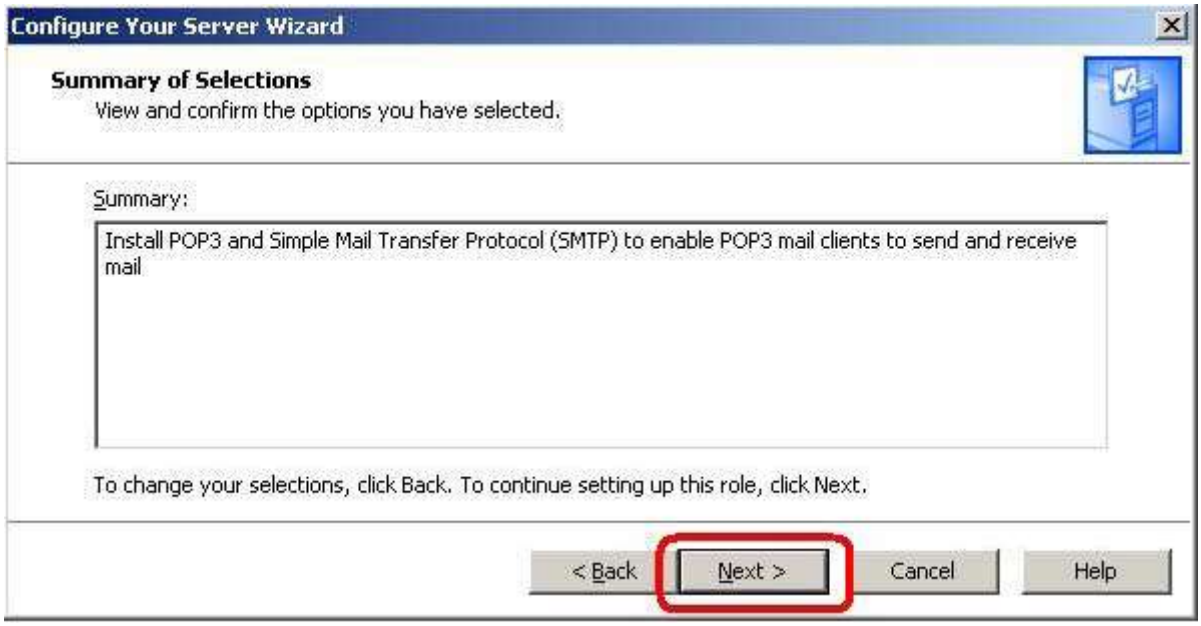


در این صفحه بر روی Mail Server (POP3 , SMTP) کلیک کرده و بر روی دکمه Next کلیک نمایید تا این نقش بـه نقـش های سرور اضافه شود.

در مرحله بعدی نام Host مورد نظر خود را وارد کرده و سپس بر روی Next کلیک می کنیم. بهتر است نام Host را همان نام دامنه خود وارد نمایید. سپس روی Next کلیک کنید.



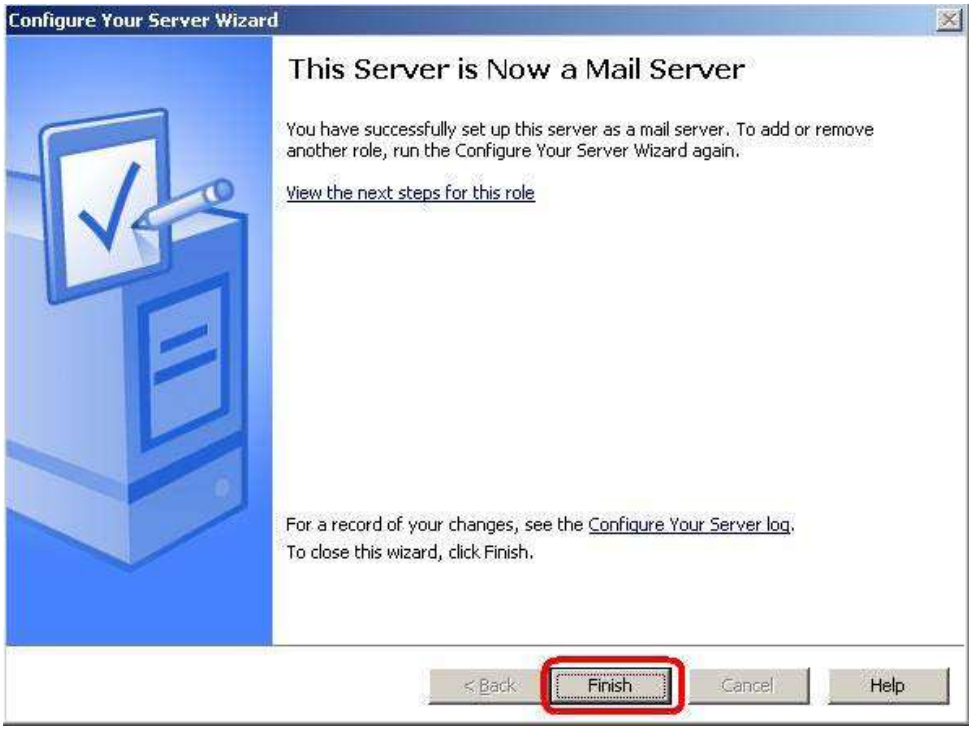
در این صفحه بر روی Next کلیک کنید.



پس از کلیک بر روی دکمه Next، صفحه زیر ظاهر می شود:

پس از این مرحله نصب آغاز می شود و معمولاً نیاز به CD ویندوز سرور ۲۰۰۳ می باشد.

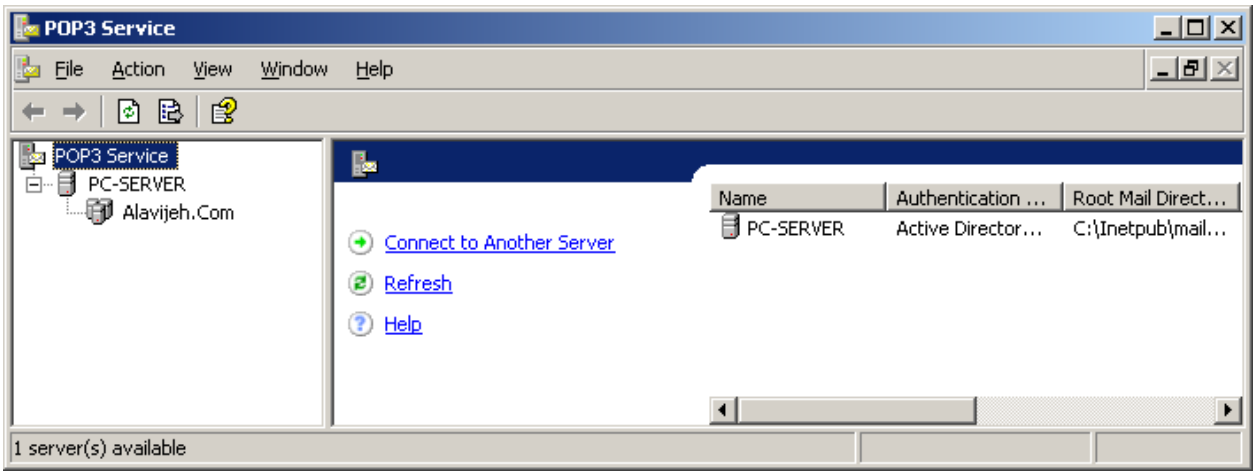
پس از پایان عملیات نصب صفحه اتمام نصب مشاهده می گردد که نشان می دهد Mail Server با موفقیت نصب شده است.



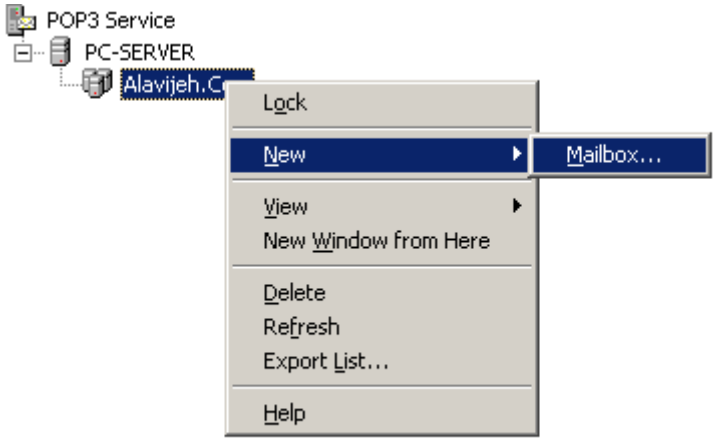
۲۶-۲- اجرای Mail Server

برای اجرا مانند شکل زیر از مسیر Administrative Tools ➔ Start، بر روی POP3 Service کلیک کنید تا برنامه سـرویس ایمیل اجرا گردد.

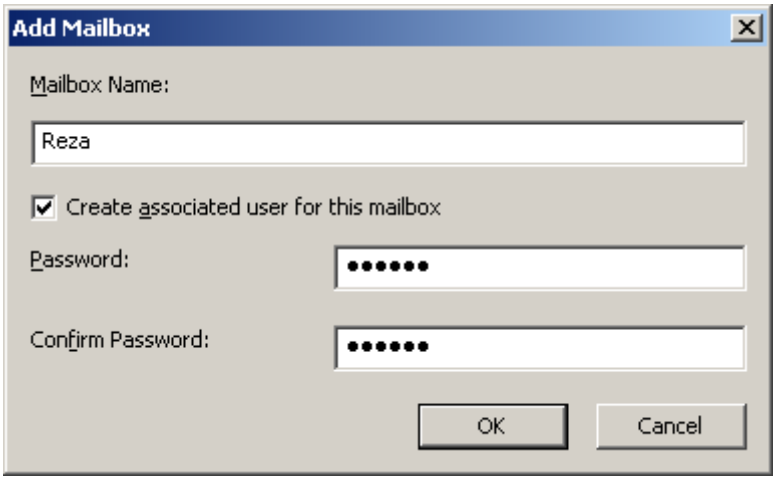
پس از اجرای Mail Server، صفحه زیر ظاهر می شود که نام Server و نام Host مورد نظر در آن قابل مشاهده می باشد.



برای ایجاد یک ایمیل جدید بر روی Host کلیک راست کرده و سپس بر روی MailBox ➔ New کلیک کنید.



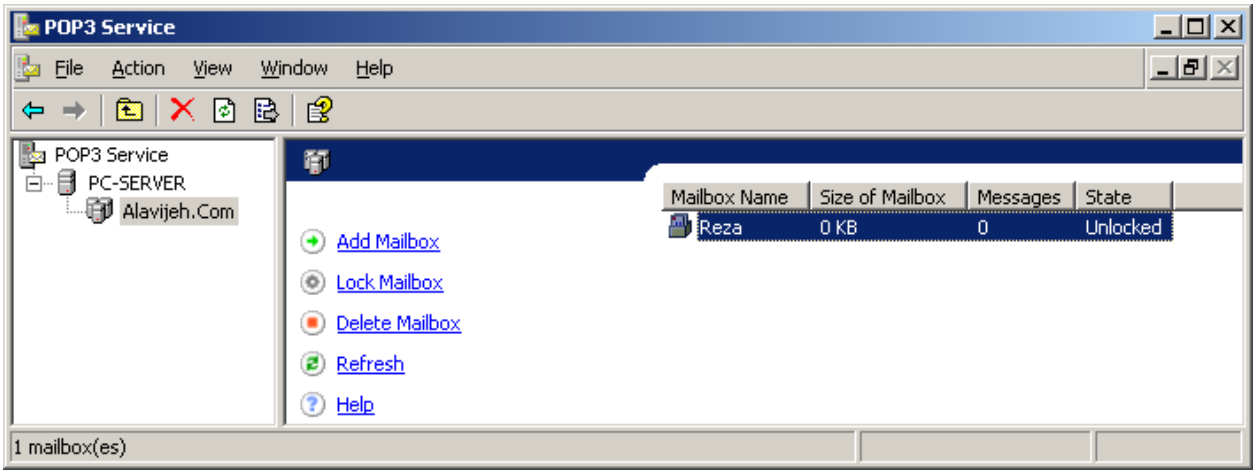
سپس صفحه ای ظاهر می شود که در آن باید نام ایمیل و کلمه عبور را وارد نمائید.



پس از کلیک بر روی OK، ایمیل جدید، مانند شکل زیر ظاهر می شود که شما می توانید تعداد ایمیل های بی شماری بر روی Hostهای مختلف ایجاد نمائید.

همانند شکل فوق پس از کلیک بر روی OK، پیغامی ظاهر می شود که اطلاعات مربوط به Account ایمیل ایجاد شده را نشان می دهد

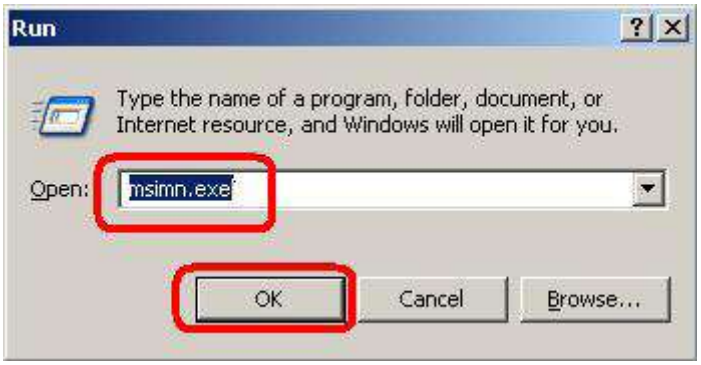
در این بخش شما می توانید ایمیل باکس ایجاد شده را نیز مدیریت نمائید. البته این بخش شامل یک سری دستورات و امکانات عمومی می باشد.



تا این مرحله Mail Server نصب شده است. حال نیاز به برنامه ای داریم که بتوانیم ایمیل ارسال و دریافت نماییم. برای این از نرم افزار Outlook Express استفاده می کنیم.

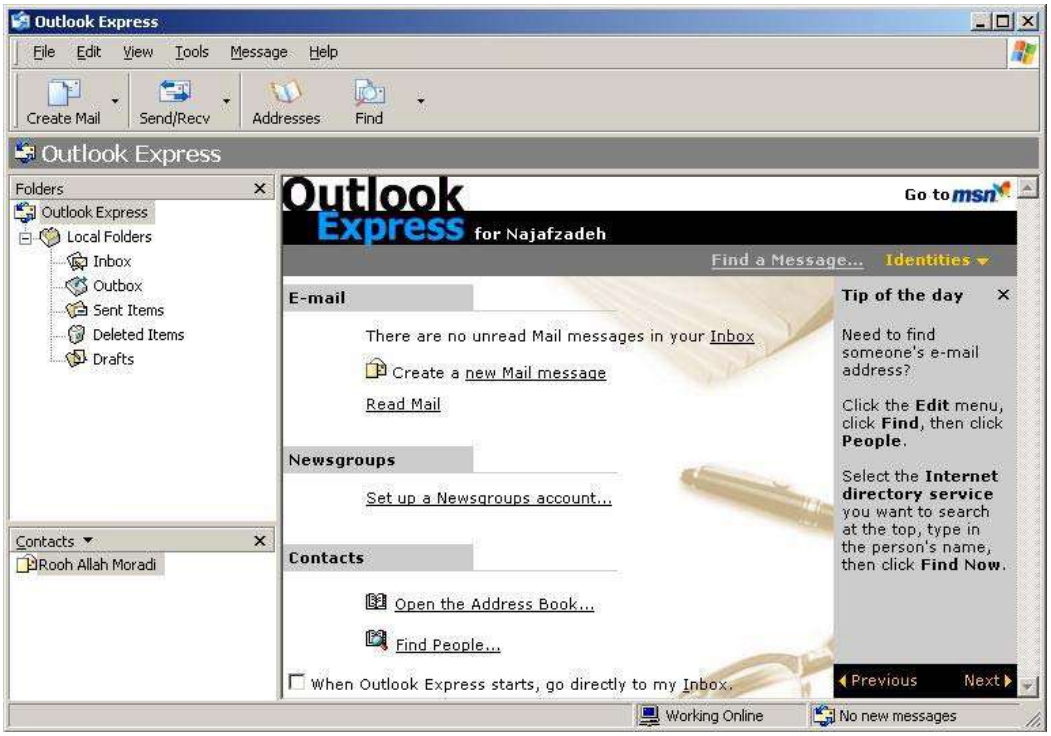
۲۶-۳- ارسال و دریافت ایمیل با استفاده از Outlook Express

برای اجرا و پیکربندی نرم افزار Outlook Express، در قسمت Run، دستور msimn.exe را نوشته و آن را اجرا کنید.

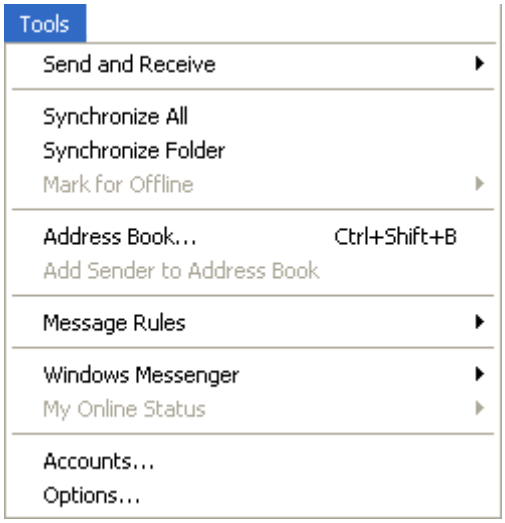


البته امکان باز کردن این نرم افزار به صورت مستقیم و از نوار Start وجود دارد.

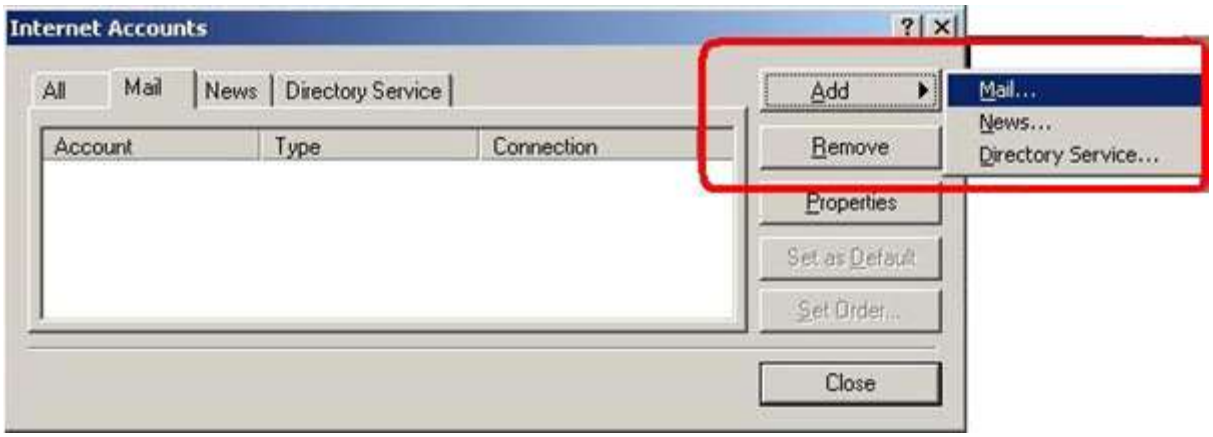
با این کار، نرم افزار Outlook Express اجرا می شود و شکل زیر ظاهر می شود:



در این بخش باید از منوی Tools گزینه Accounts را انتخاب نماییم.

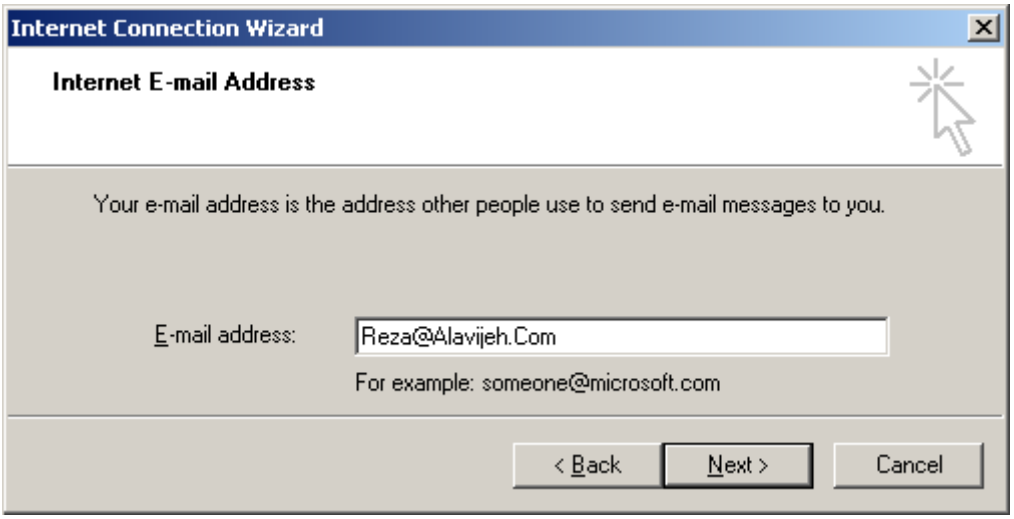


سپس صفحه زیر ظاهر می شود که باید در آن در سربرگ Mail، گزینه Add ➔ Mail را انتخاب نمایید.

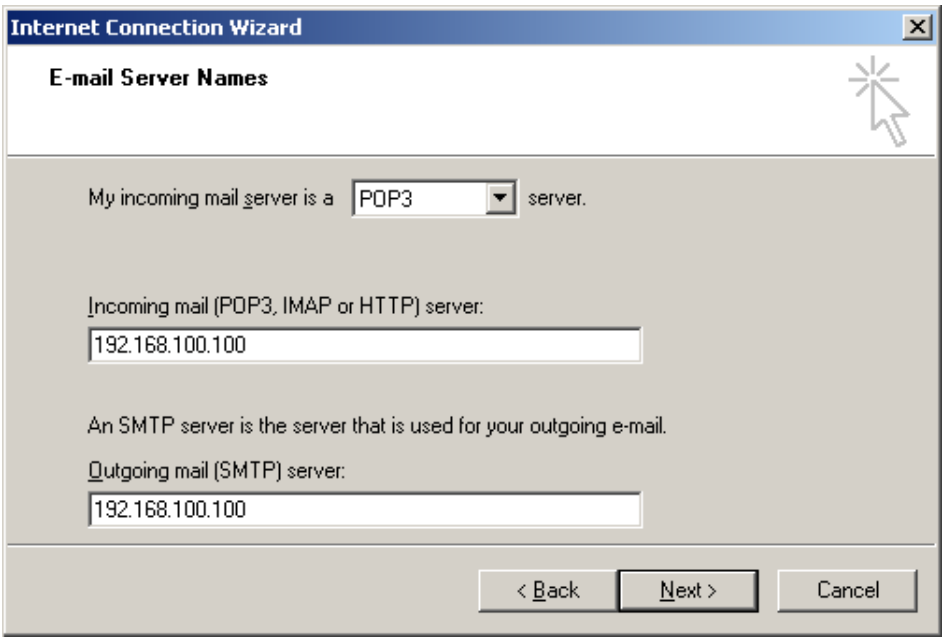


در مرحله بعد، نامی که به جای آدرس ایمیل (مثلاً نام صاحب ایمیل) نمایان خواهد شد را وارد نمایید.

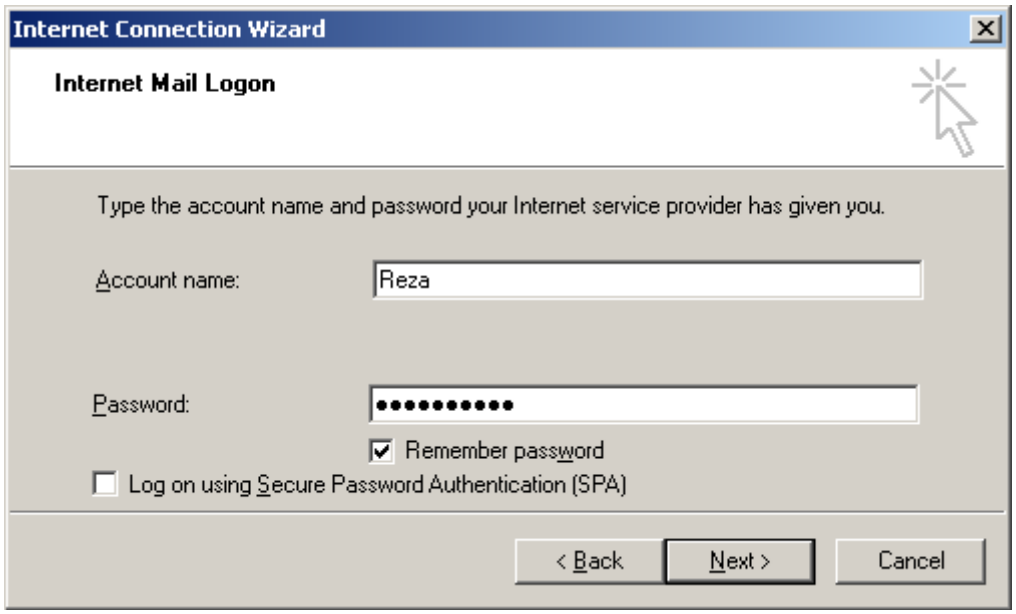
در مرحله بعدی آدرس ایمیل را به صورت کامل وارد کنید.



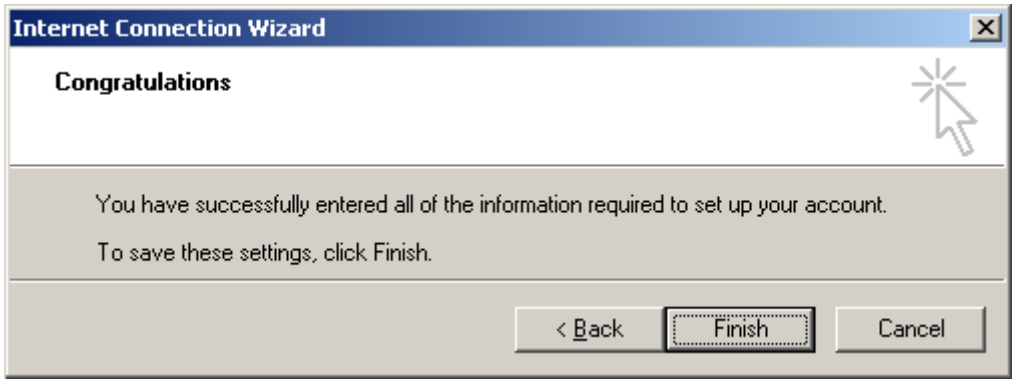
در مرحله بعدی باید تنظیمات SMTP و POP3 را انجام دهید. می توانید از آدرس IP یا نام سرور مورد نظر استفاده نمایید.



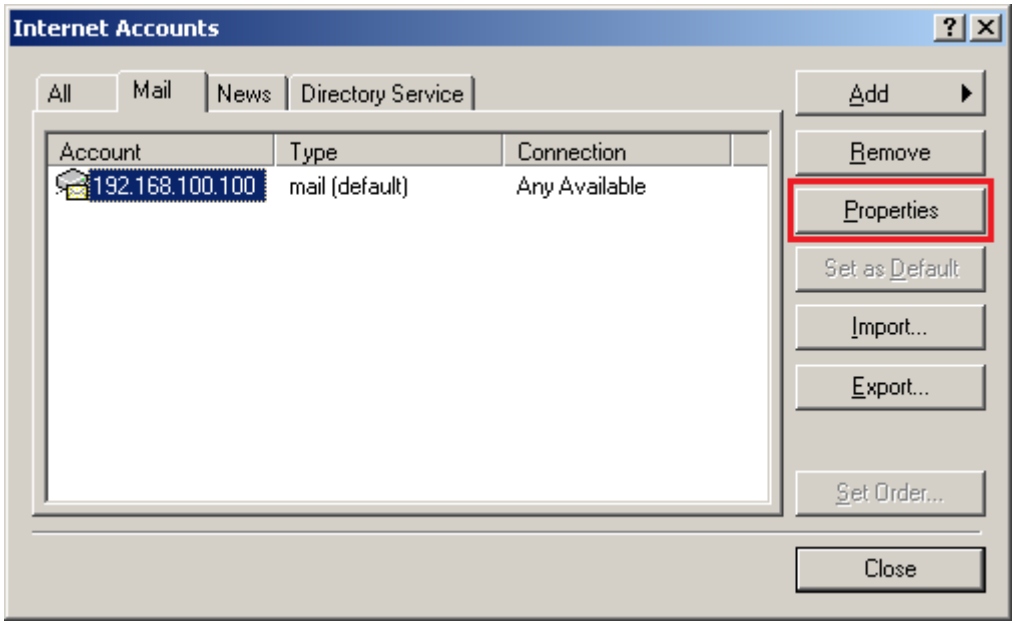
در مرحله بعدی، نام کاربری و کلمه عبور را وارد نمایید. توجه نمایید که نام کاربری ما در حقیقت آدرس کامل ایمیل می باشد.



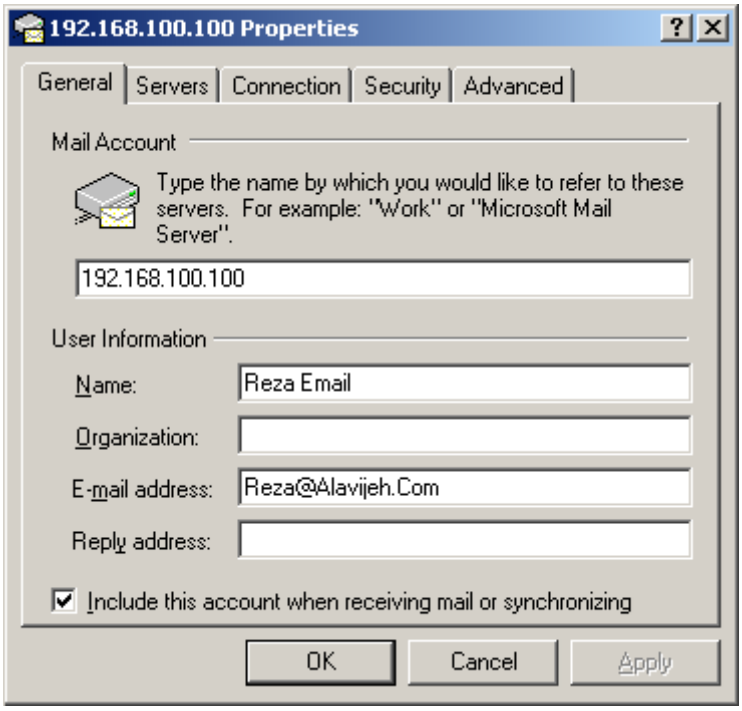
پس از این مرحله بر روی Finish کلیک کنید.



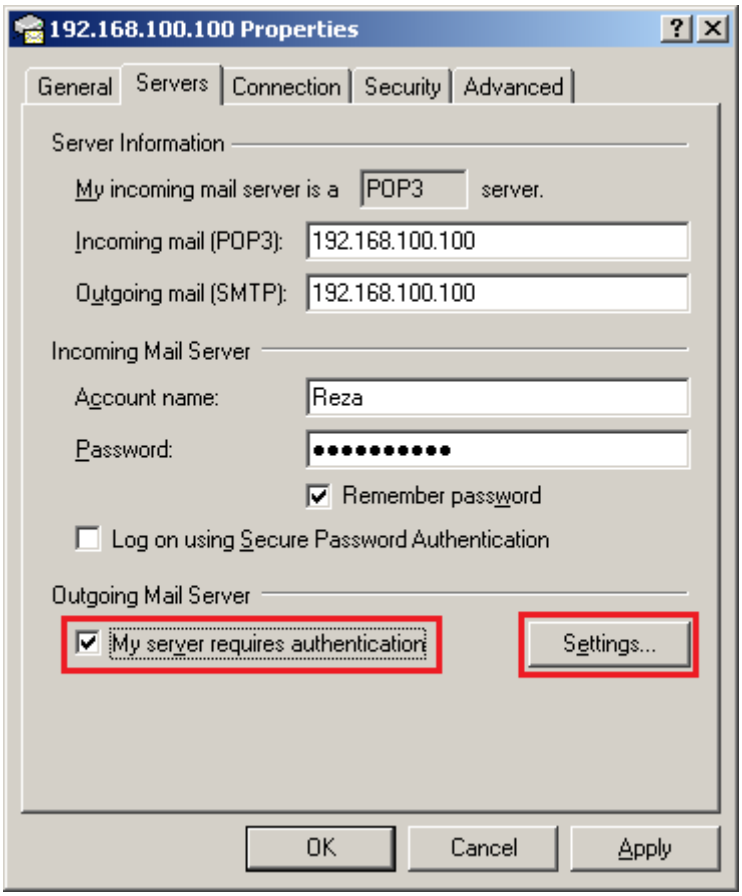
سپس مجددا به بخش Account وارد شده، بر روی آدرس ایمیل ساخته شده در بخش Mail کلیک نموده و در بخش سمت راست صفحه بر روی Properties کلیک می کنیم.



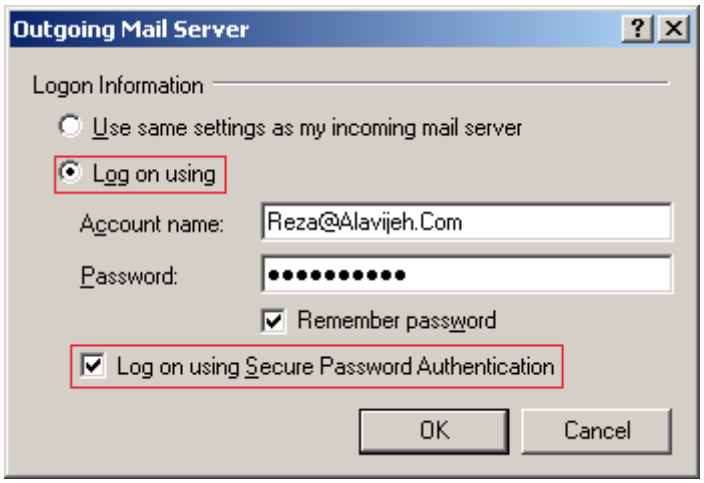
صفحه ای ظاهر می شود که در آن بر روی Servers کلیک می نماییم و تنظیمات دیگری را نیز انجام می دهیم.



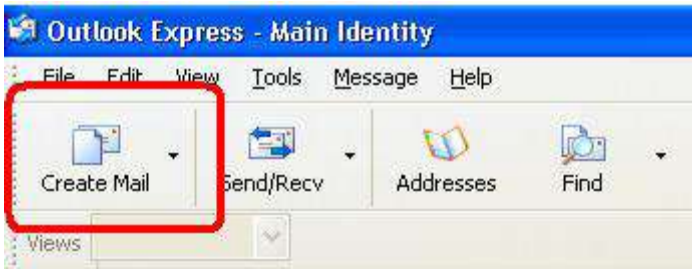
در ابتدا تیک مربوط به بخش My Server Requires authentication را زده و سپس بر روی دکمه Setting کلیک کنید.



سپس صفحه زیر ظاهر شده که باید نام کاربری و کلمه عبور را یک بار دیگر وارد نموده و سپس تیک گزینه Logon using Secure Password Authentication را می زنیم. توجه نمایید که در این بخش هم نام کاربری و هم نام دامنه (یعنی Alavijeh.Com) را وارد نمایید. سپس بر روی کلید OK کلیک کرده و از این بخش نیز خارج می شویم.

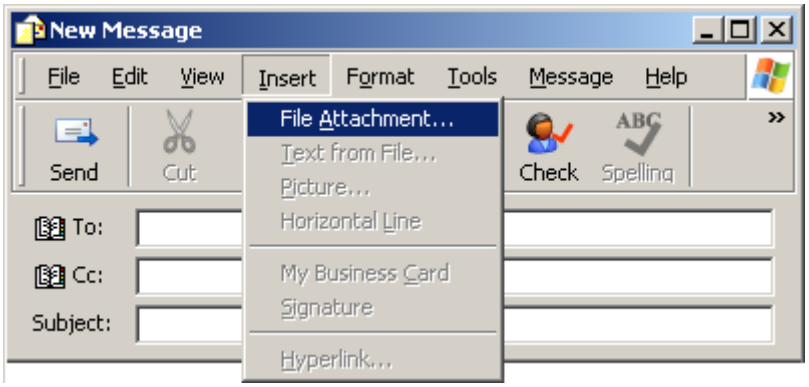


جهت ارسال ایمیل در Outlook Express، بر روی Create Mail کلیک کنید.

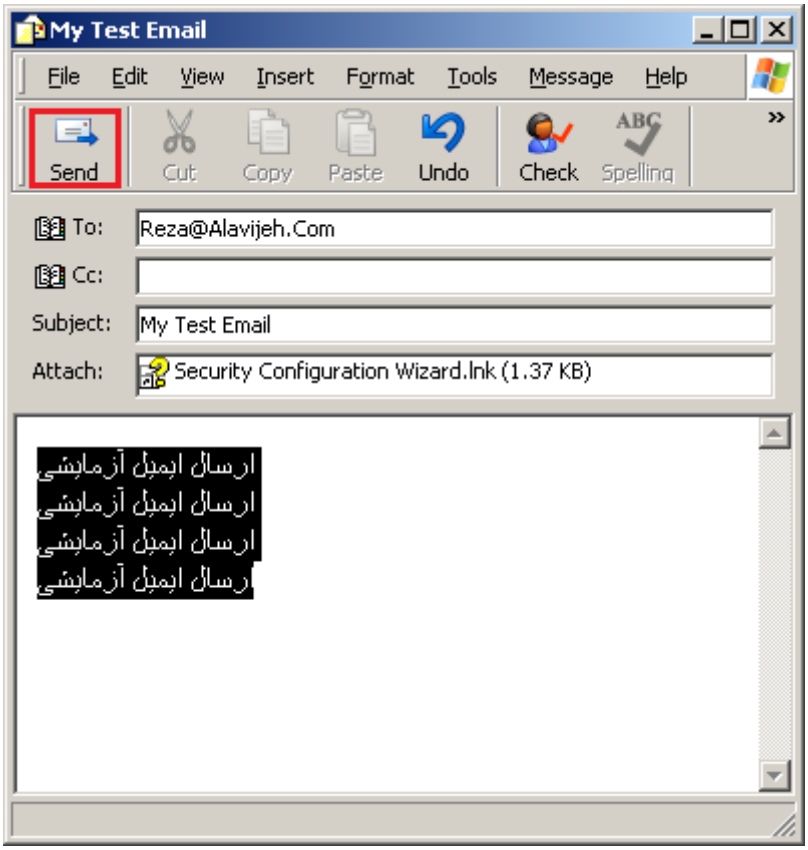


پس از این مرحله یک ایمیل خالی به شکل زیر ظاهر می شود که باید ایمیل گیرنده را و ارد نمود.

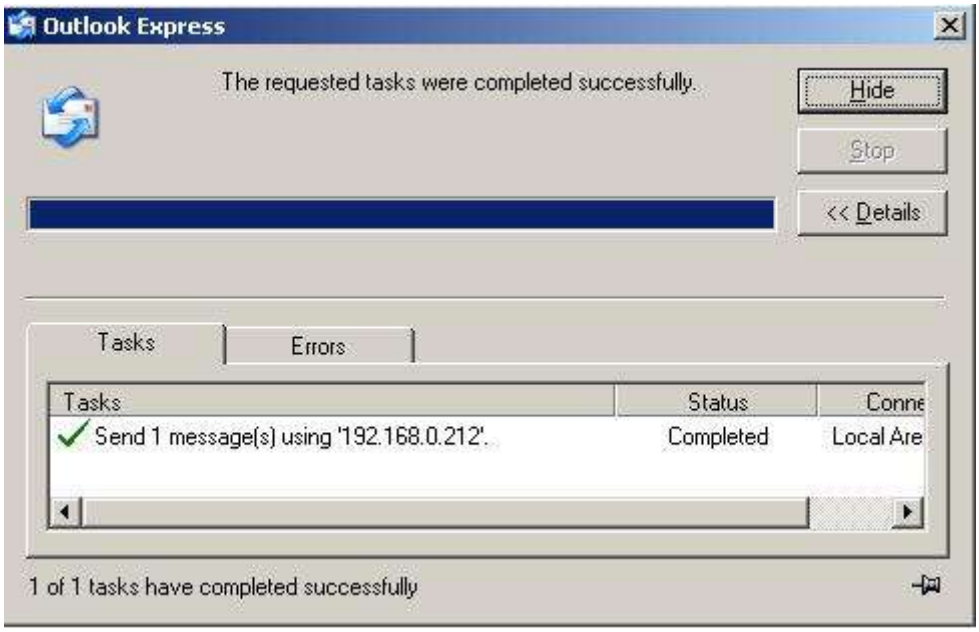
جهت ضمیمه نمودن فایلی خاص، از منوی Insert، گزینه File Attachment را انتخاب نمایید.



پس از وارد کردن اطلاعات مورد نیاز (ایمیل گیرنده، عنوان ایمیل، متن ایمیل، فایل های ضمیمه و ...) بـر روی Send کلیـک کنید. در قسمت To، ایمیل گیرنده اصلی نامه و در قسمت Cc، ایمیل افرادی را وارد نمایید که یک رونوشت از ایمیل اصلی را دریافت می کنند. اعضای قسمت To متوجه می شوند که ایمیل برای چه کسانی در قسمت Cc ارسال شده است.

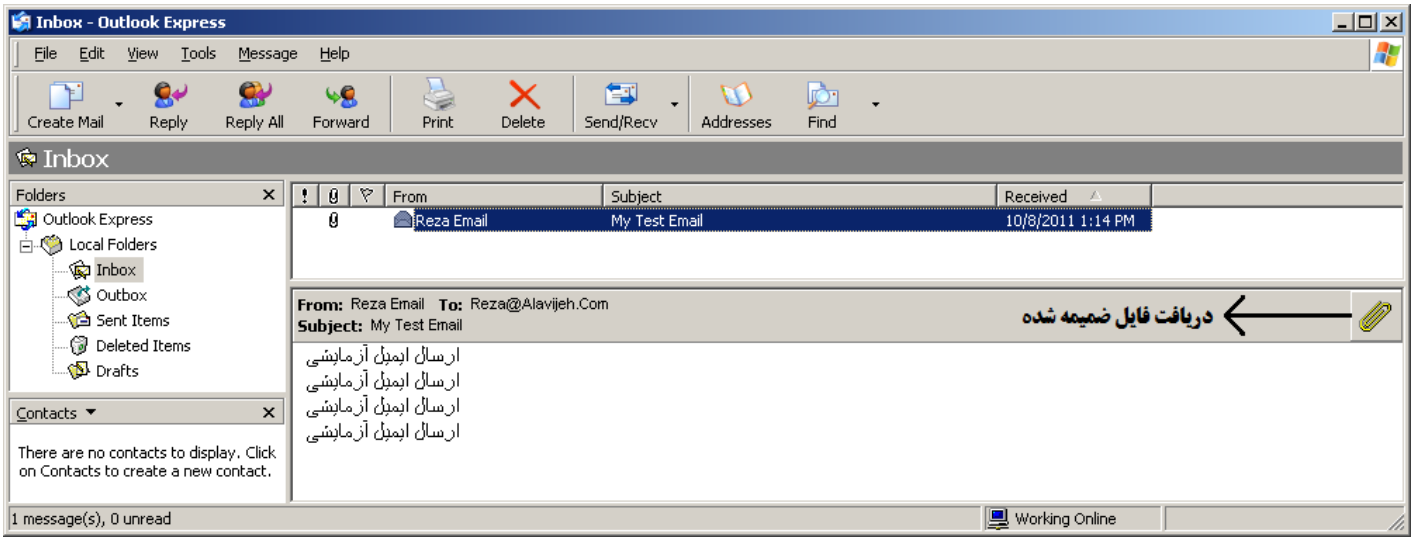


پس از ارسال شکل زیر در صورتی که ایمیل با موفقیت ارسال شود شکل زیر ظاهر می شود:



برای دریافت ایمیل نیز کافیست بر روی Send/Receive کلیک نمایید.

در صورتی که تنظیمات درست انجام شده باشد و ایمیلی در Inbox ما موجـود باشـد، توسـط Outlook Express بـه صـورت خودکار، به سیستم خودمان واکشی می شود.



فصل ۲۷

FTP Server

به عنوان یک کاربر خانگی، ممکن است بارها برایتان پیش آمده باشد که بخواهید تعدادی از فایل های خود را در مدت زمانی نامحدود در دسترس دیگران قرار دهید؛ اما به دلایلی نمی خواهید که پوشه Share شده ای در سیستم تان وجود داشته باشد و یا شاید یک مدیر سیستم هستید که دفاتر متعددی در نقاط مختلف یک شهر یا یک کشور دارید و استفاده از فایل های مشترکی برای همه دفاتر الزامی به نظر می رسد اما حجم و محدودیت های شبکه امکان ارسال آنها را با پست الکترونیکی فراهم نمی کند؛ اصلاً شما می خواهید این دسته از فایل ها همیشه در یک جای ثابت برای دریافت در دسترس باشند و دائم مجبور نباشید برای تک تک دفاتر آنها را ارسال کنید. یک راه حل ساده، سریع و قدیمی برای این کار راه اندازی یک FTP Sever است. شما می توانید بر روی ویندوز XP Professional خانگی خود یا یکی از سرورهای محل کار به سادگی و در عرض چند دقیقه یک سرویس انتقال فایل راه اندازی کنید. پروتکل FTP یا File Transfer Protocol یکی از پروتکل های لایه کاربرد (Application) در معماری TCP/IP است که مسئولیت انتقال فایل ها را تحت شبکه بر عهده می گیرد، برنامه سرویس دهنده FTP از **پورت TCP شماره ۲۰ یا ۲۱** استفاده می کند که با استفاده از پروتکل TCP اقدام به انتقال فایل بین سیستم های مبتنی بر ویندوز و یک سرویس دهنده FTP ویندوزی می کند. با اینکه برخی از توانائی های این سرویس توسط سرویس وب (www) نیز ارائه می شود اما هنوز استفاده از سرویس FTP رواج دارد. به طور کلی به علت مسایل امنیتی سعی می شود که امکان ارسال فایل توسط همه کاربران غیر ممکن گردد و تنها عده خاصی با داشتن نام کاربری و رمز عبور قادر به ارسال فایل بر روی FTP Server باشند.

یک FTP Server می تواند سرویس دهنده ای بسیار کارآمد باشد، در عین اینکه عدم نظارت و کنترل آن ممکن است نقطه ضعفی برای سیستم به شمار آید.

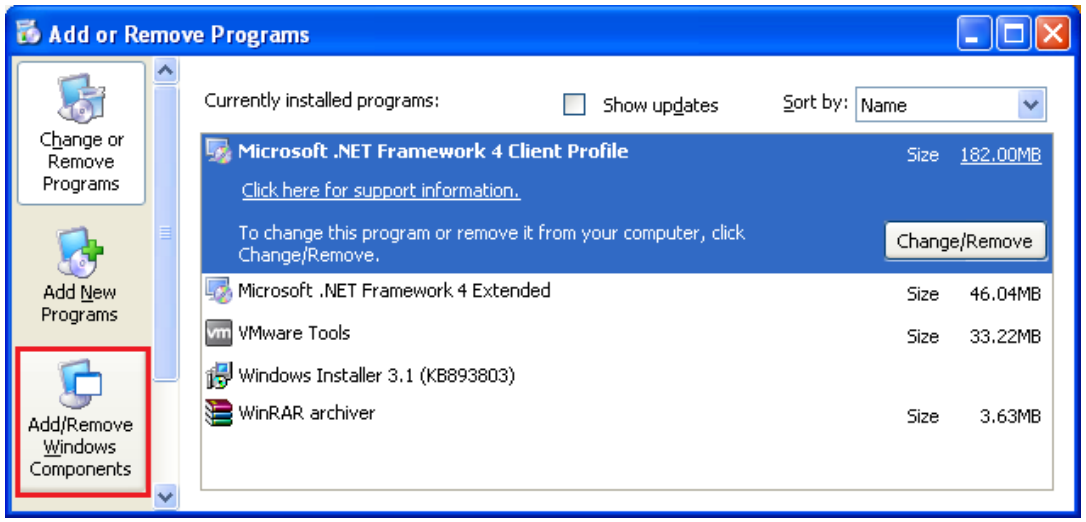
FTP با شماره پورت ۲۱، یک پروتکل قدیمی است و کاربرد آن به زمانی بر می گردد که استفاده از پورت ۸۰ (WEB) نیز چندان فراگیر نشده بود. زمانی می توان از یک کامپیوتر (با سیستم عامل XP، 2000 یا سرور ۲۰۰۳) خدمات FTP دریافت نمود که این سرویس روی آن سیستم عامل فعال شده باشد یعنی یک FTP Server روی سرور مورد نظر در حال کار باشد. بعد از برقراری ارتباط با FTP Server در حقیقت شما به یک FTP Client تبدیل می شوید.

بوسیله این پروتکل می توان فایل ها را در سرویس دهنده Upload نیز کرد اما برای قرار دادن فایل در طرف سرویس دهنده بایستی هر کاربر یک FTP Account داشته باشد که توسط ارائه دهنده سرویس در اختیار کاربر یا همان FTP Client قرار گرفته و به وسیله آن با توجه به حق دسترسی تعیین شده می توان به ایجاد، اضافه، حذف و یا تغییر فایل های موجود در سرویس دهنده از طریق یک دستگاه دیگر بپردازد. برای Upload کردن می توان از برنامه هایی مانند Cute FTP، Flash FXP، WS FTP و... استفاده نمود. اما در این فصل و جزوه آموزشی، قصد داریم از طریق راه اندازی FTP Server این کار را آموزش دهیم.

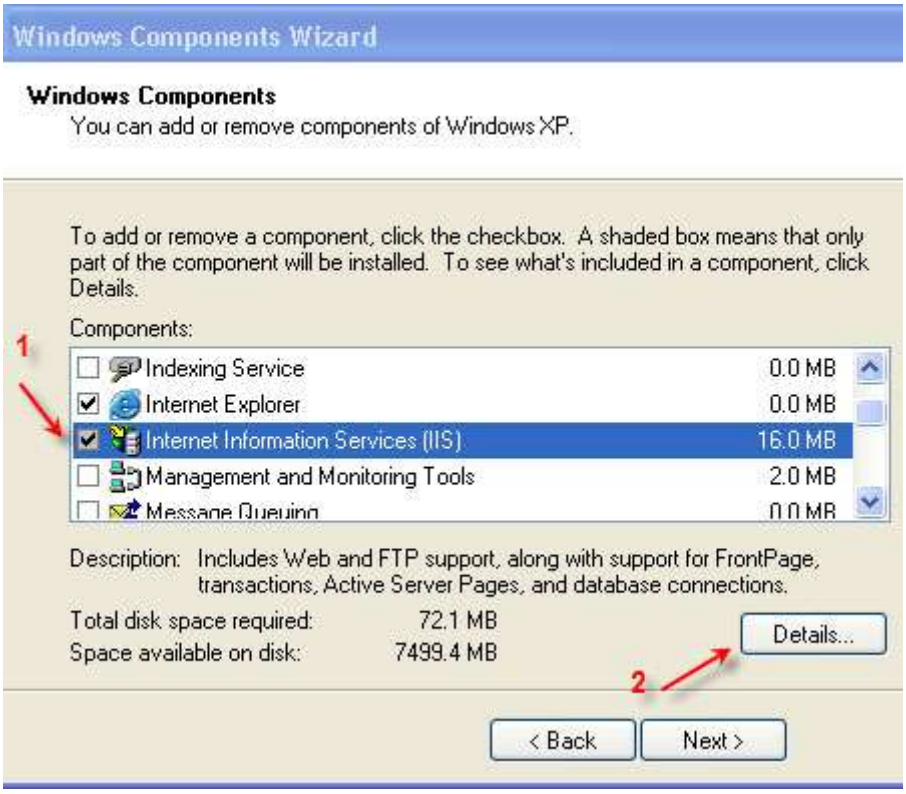
۲۷-۱- راه اندازی FTP Server

سرویس FTP یکی از سرویس های ارائه شده به همراه IIS (Internet Information Services) است که به طور پیش فرض در تمام سیستم عامل ها غیرفعال است پس بایستی آن را نصب و فعال کرد. برای این منظور در ویندوز XP مراحل زیر را طی کنید:

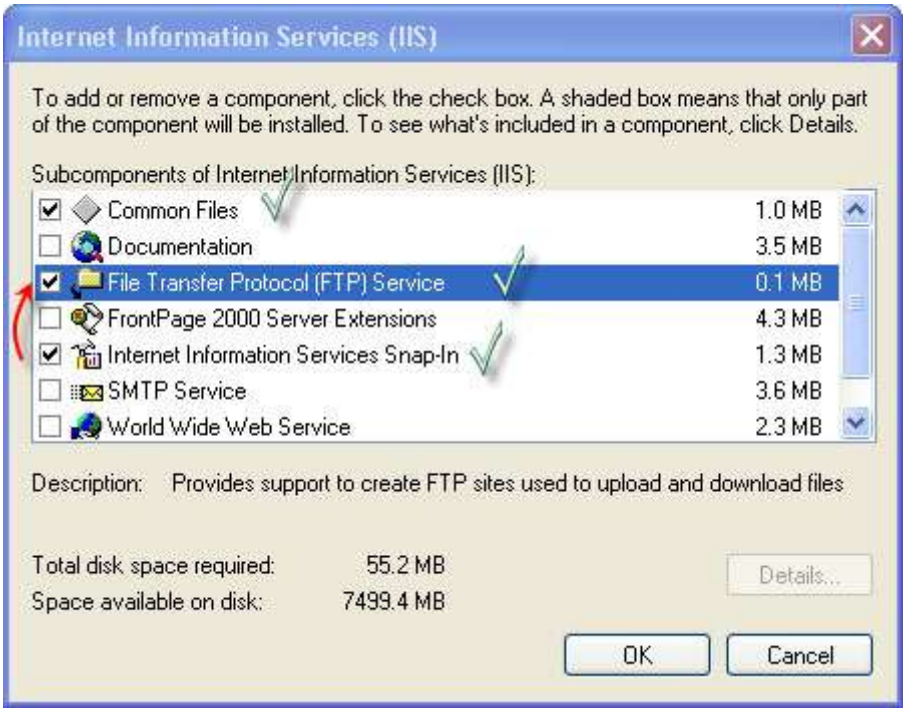
۱. Control Panel را باز و Add or Remove Program را انتخاب نمایید. در پنجره باز شده از قسمت سمت چپ، بر روی آیکون Add/Remove Windows ... را کلیک کنید.



۲. پس از چند لحظه انتظار پنجره مربوطه ظاهر می شود. در لیست Component، مانند شکل زیر در مربع کنار IIS تیک بزنید، بدون اینکه با زدن Next به مرحله بعد بروید، دکمه Details را انتخاب کنید.



۳. IIS شامل چندین سرویس است که یکی از آنها FTP است و چون هدف ما تنها نصب FTP است پس در پنجره Details، در ابتدا تیک کنار همه گزینه ها را برداشته و فقط گزینه File Transfer Protocol (FTP) Service را انتخاب کنید، که طبق شکل زیر به همراه آن، دو سرویس دیگر نیز فعال می شود. تغییری در این تنظیمات ندهید؛ OK را بزنید و با بازگشت به صفحه قبل Next را انتخاب کنید.

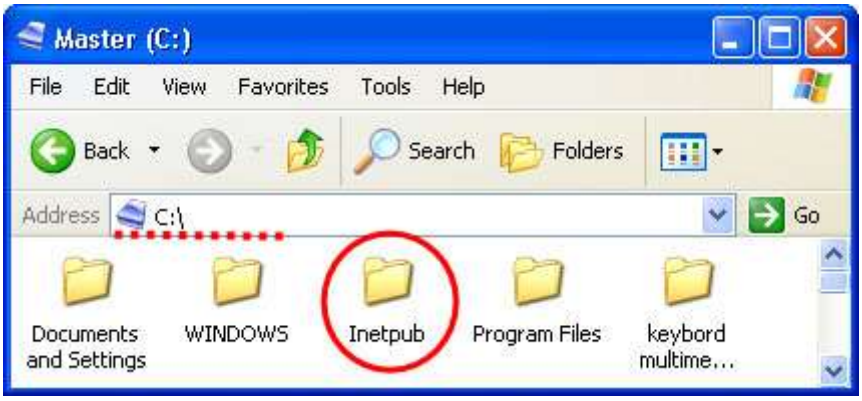


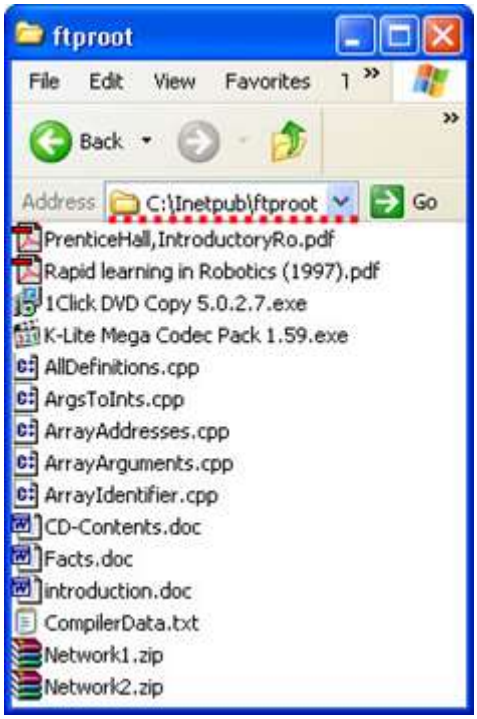
۴. در اینجا نصب سرویس شروع می شود. در اواسط روند نصب، از شما درخواست CD ویندوز می شود. پس از قراردادن CD و نصب فایل های مورد نیاز، سرویس FTP بر روی کامپیوتر فعال می گردد.

۲۷-۲- قراردادن فایل ها بر روی FTP Server

با طی شدن مراحل بالا اکنون سیستم به یک FTP Server تبدیل شده است. برای قراردادن فایل های مورد نظرتان، پوشه خاصی در نظر گرفته شده است که هر چیزی که در این پوشه قرار گیرد، سرویس دهنده آن را در لیست فایل ها و پوشه های FTP Server قرار می دهد.

همانطور که در دو شکل زیر مشاهده می کنید، به محض نصب FTP Server یک پوشه در درایو C کامپیوتر ایجاد می شود که Inetpub نام دارد. درون این پوشه نیز دو پوشه دیگر به نام های ftproot و AdminScripts قرار دارد، پوشه مورد بحث ما که محل قرارگیری فایل های FTP Server است ftproot است. حالا همه چیز آماده قرارگیری فایل ها است. فایل هایتان را در این مکان قرار دهید، هم اکنون شما یک FTP Server آماده استفاده دارید.





۲۷-۳- اتصال به FTP Server

مسلما یک FTP Client ابتدا باید به FTP Server متصل گردد تا بتواند از خدمات آن استفاده کند در یک شبکه داخلی این امر با تایپ یکی از دو نوع آدرس زیر در نوار آدرس IE یا هر Web Browser دیگری مثل Mozilla میسر می شود و کاربران شبکه با داشتن IP Address یا نام کامپیوتر سرویس دهنده FTP، می توانند لیست فایل های موجود در آن را مشاهده و سپس نسبت به دریافت اقدام کنند.

ftp://FTP Server **IP address** یا ftp://FTP Server **Computer Name**

اما کاربرانی وجود دارند که می خواهند از این سرویس توسط نوع دیگری از ارتباط استفاده کنند بدین معنی که هدف آنها از راه اندازی این سرویس در دسترس قرار دادن فایل هایی برای افراد خاصی است که با اجازه آنها قادر به اتصال به سیستم باشند. نحوه ساختن این نوع ارتباط بدون نیاز به اینترنت و توسط مودم صورت می گیرد که به طور کامل در فصول قبل توضیح داده شده است؛ لذا از تکرار آن خودداری می کنیم.

طبق شکل زیر، ما لیستی از فایل ها را در پوشه ftproot قرار دادیم. فرض کنید آدرس IP ما، برابر با ۱۶۹.۲۵۴.۱۹۵.۱۵۷ باشد.

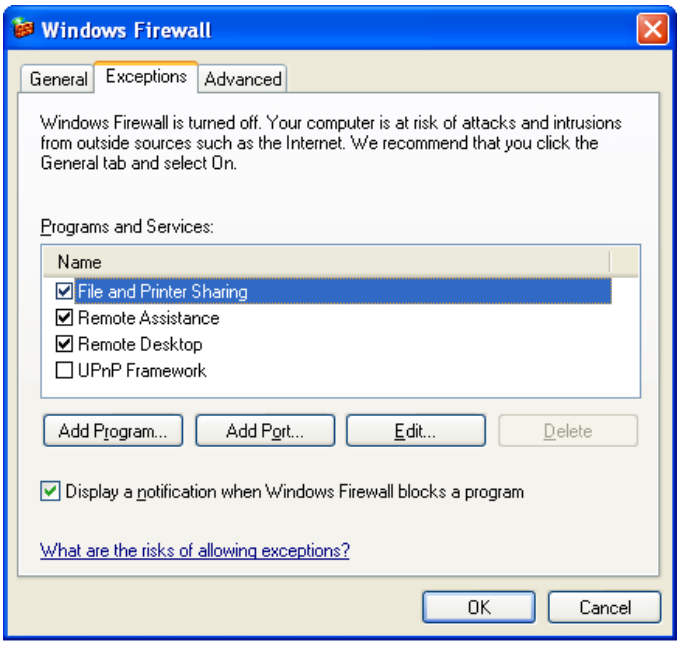
FTP Client مورد نظر مانند شکل زیر، این آدرس IP را در نوار آدرس مرورگر Mozilla وارد و سپس همان لیست را که در شکل فوق وجود داشت به صورت لینک های قابل Download می بیند. به همین راحتی!! کار ما تمام شد. از این به بعد شما تنها به ویرایش لیست تان می پردازید و دیگر لازم نیست پوشه ای را Share کنید و یا فایل ها را با درد سر Email کنید.

سرعت بالاتر و نظم موجود در این سرویس از مزایای آن به شمار می رود. نکته قابل توجه دیگر اینکه، با وجود یک نرم افزار مدیریت Download مثل IDM یا DAP می توان فایل های حجیم را هم با سرعت بالاتری منتقل کرد.

با هر نوع Connection که به سرور متصل شده باشید چه از طریق شبکه داخلی یا اینترنت و یا روشی که ما به شما ارائه کردیم امکانات FTP در اختیار شماست.

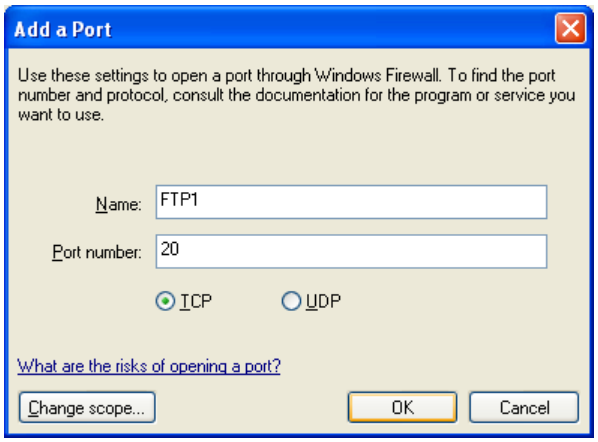
۲۷-۴- تنظیم Firewall

این مسأله را فراموش نکنید که در صورتیکه فایروال سیستم شما فعال باشد نمی توان به سرویس دهنده FTP شما متصل شد، پس بایستی آن را غیرفعال کنید. البته می توان این مشکل را با غیر فعال نکردن Firewall نیز حل کرد. راه حل این است که پورت های ۲۰ و ۲۱ را به Firewall خود معرفی کنید (همان دو پورتی که FTP Server برای خواندن و نوشتن از آن استفاده می کند). بدین منظور، ابتدا وارد Control Panel ➔ Windows Firewall شده و سپس وارد سربرگ Exceptions شوید.

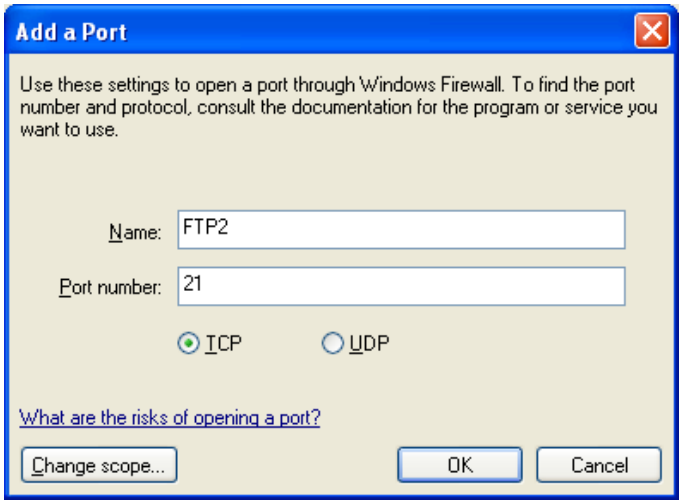


سپس روی دکمه Add Port کلیک کنید.

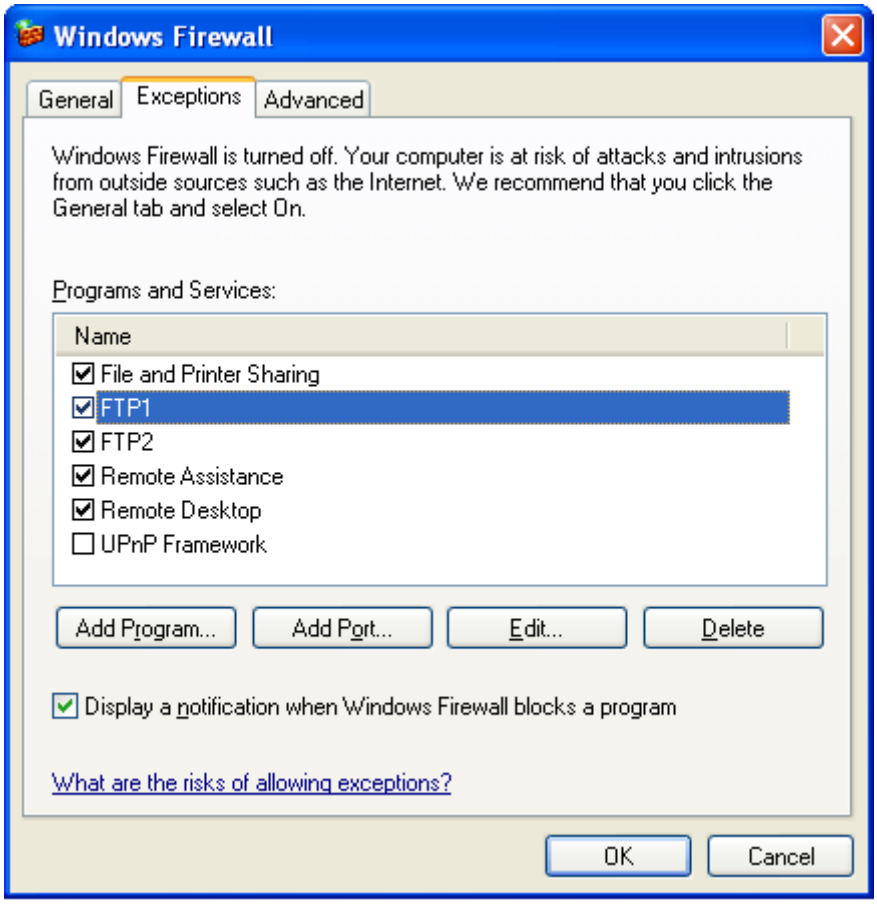
سپس در صفحه باز شده، پورت ۲۰ را با نام FTP1 اضافه کنید.



مجددا روی Add Port کلیک کنید. اینبار پورت ۲۱ را با نام FTP2 اضافه کنید.



با OK کردن، این دو پورت، به مجموعه پورت های ویندوز که Firewall جلوی آن ها را نمی گیرد، اضافه خواهد شد.


Windows Firewall
General
Exceptions
Advanced
Windows Firewall is turned off. Your computer is at risk of attacks and intrusions from outside sources such as the Internet. We recommend that you click the General tab and select On.
Programs and Services:
Name
File and Printer Sharing
FTP1
FTP2
Remote Assistance
Remote Desktop
UPnP Framework
Add Program...
Add Port...
Edit...
Delete
Display a notification when Windows Firewall blocks a program
What are the risks of allowing exceptions?
OK
Cancel

فصل ۲۸

Microsoft Management Console یا MMC

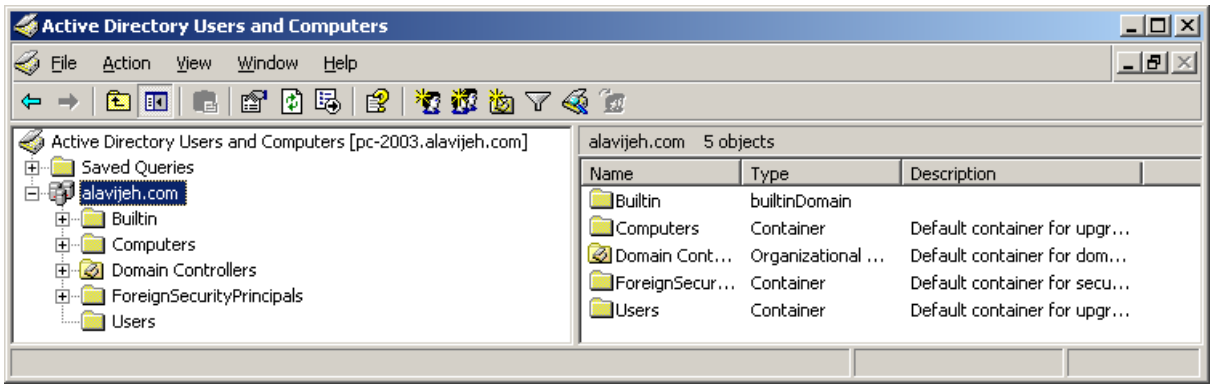
۲۸-۱- مفهوم Microsoft Management Console

شاید برای شما هم اتفاق افتاده باشد که مجبور شده باشید کارهایی متعدد و تکراری را هر روز با کامپیوتر انجام دهید. در این وضعیت ما ۳ حالت را بررسی می کنیم. اولا برای شما خوشایند خواهد بود که به سرعت به نرم افزارهای مربوط به این کارها به سرعت دسترسی پیدا کنید. ثانیا اگر طراحی نرم افزارها به گونه ای باشد که ظاهری شبیه یکدیگر داشته و همگی از یک استاندارد طراحی پیروی کنند، این امر باعث خواهد شد که با دیگر نرم افزارها بتوانید به سادگی کار کنید. به عنوان مثال وقتی در ویندوز، با دو بار کلیک روی یک پوشه می توانید آن را باز کنید، انجام این کار در لینوکس نیز برای شما راحت خواهد بود. اما اگر تاکنون فقط با سیستم عامل Dos کار کرده باشید و بخواهید مستقیماً به سراغ محیط گرافیکی لینوکس بروید، احتمالا دچار مشکل خواهید شد. ثالثا، ممکن است شما به عنوان مدیر شبکه، نیاز داشته باشید که هر روز **قسمت های مدیریتی** برخی یا تمام کامپیوتر های موجود در شبکه را کنترل نمایید. برای این کار مجبورید که شخصا پشت هر کامپیوتر بروید و آن قسمت مدیریتی را بررسی نمایید. اما چقدر خوب می شود که بتوان از راه دور، قسمت های مدیریتی تمام سیستم ها را کنترل نمود. ممکن است بگویید که می توان این مشکل آخر را با نرم افزار Remote Desktop حل کرد. اما این روش دو عیب دارد: اول اینکه Remote Desktop تمام اطلاعات کامپیوتر راه دور را به کامپیوتر شما می آورد؛ لذا ترافیک شبکه بسیار بالا می رود؛ درحالی که ما به تمام قسمت های کامپیوتر راه دور نیازی نداریم و تنها به **قسمت های مدیریتی** آن نیاز داریم. عیب دوم اینکه برای کار با Remote Desktop نیاز به نام کاربری و رمز عبور کامپیوتر راه دور داریم؛ و این امر نیز خود مشکلی بزرگ است.

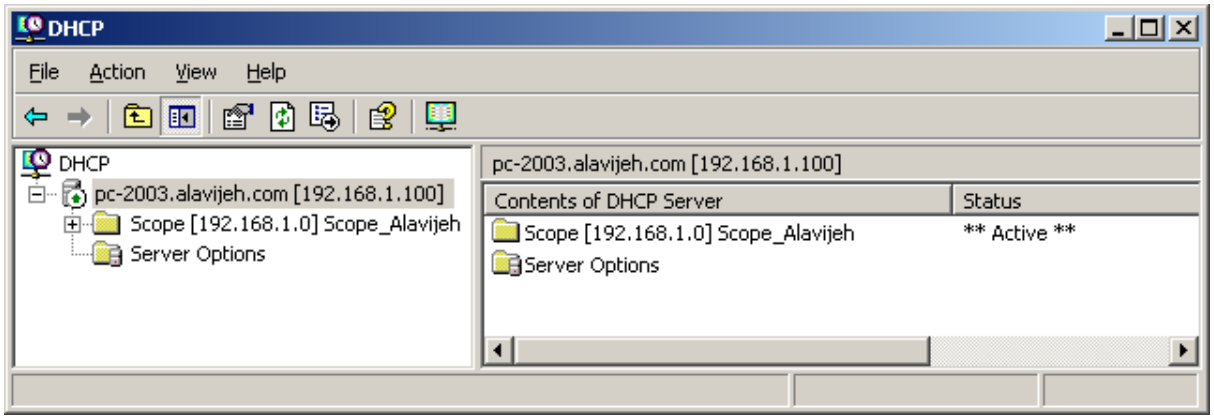
توجه نمایید که در این بخش هدف ما، اتصال به **قسمت های مدیریتی** کامپیوتر است نه فایل ها و پوشه های کامپیوتر. منظور از قسمت های مدیریتی، بخش هایی چون AD Users & Computers، DHCP، DNS، Computer Management و... است.

برای حل این مشکلات، مایکروسافت تکنیکی را تحت عنوان Microsoft Management Console یا به اختصار MMC را معرفی کرده است. MMC برای حل این مشکلات، اقدامات زیر را انجام می دهد: اولا می توان چندین قسمت مدیریتی را در کنار یکدیگر قرار داد و به راحتی در یک لحظه به همه آن ها دسترسی داشت. ثانیا، مایکروسافت شکل یکسانی را برای تمامی **قسمت های مدیریتی** طراحی کرده است. لذا کار کردن با آن ها راحت است. ثالثا توسط MMC این قابلیت وجود دارد که بتوان به کامپیوتر های راه دور بدون نیاز به نام کاربری و رمز عبور متصل شد و **قسمت های مدیریتی** را تغییر داد. برای اینکه، بهتر متوجه بحث فوق شوید، به تصاویر زیر دقت نمایید:

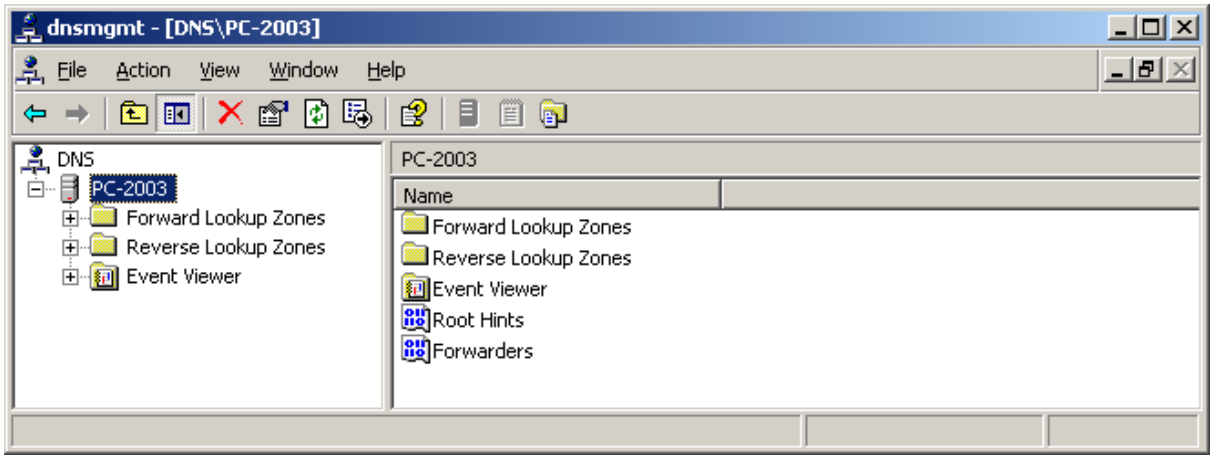
شکل زیر، کنسول مدیریتی Active Directory Users and Computers را نشان می دهد:



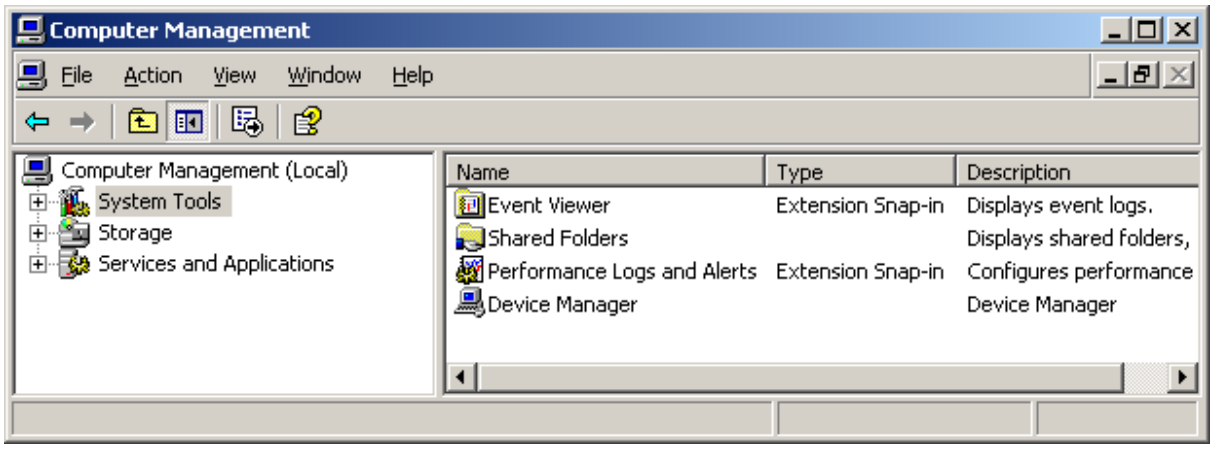
شکل زیر، کنسول مدیریتی DHCP را نشان می دهد:



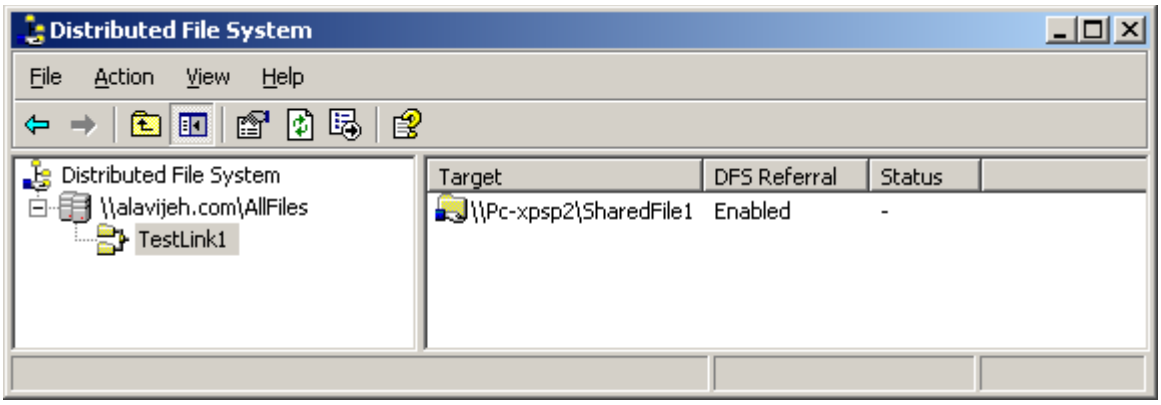
شکل زیر، کنسول مدیریتی DNS را نشان می دهد:



شکل زیر، کنسول مدیریتی Computer Management را نشان می دهد:



شکل زیر، کنسول مدیریتی Distributed File System را نشان می دهد:

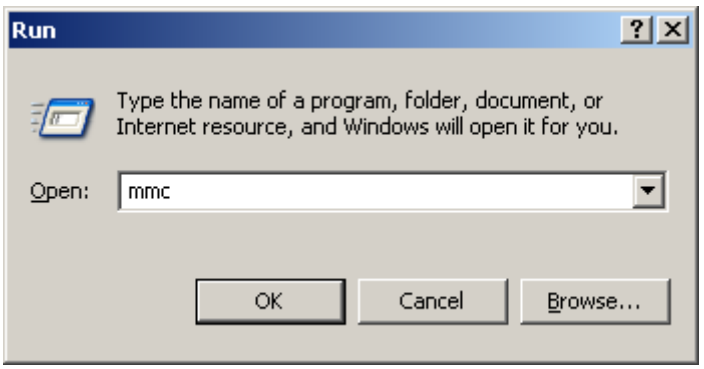


اگر دقیقا به شکل های فوق دقت کرده باشید، متوجه خواهید شد که ساختار و ظاهر طراحی آن ها به یک شکل است. بدین صورت که در سمت چپ یک ساختار سلسله مراتبی و درختی از عناصر طراحی و مدیریتی وجود دارد. با انتخاب هر کدام، زیر مجموعه های آن در سمت راست نمایان شده و می توان آن ها را تغییر داد. مایکروسافت تلاش نموده است که تمام کنسول های مدیریتی آن از این روش طراحی استفاده کنند؛ لذا با این عمل، مشکل دومی که در بالا مطرح کردیم حل می شود. حال نوبت به مشکل اول و سوم می شود.

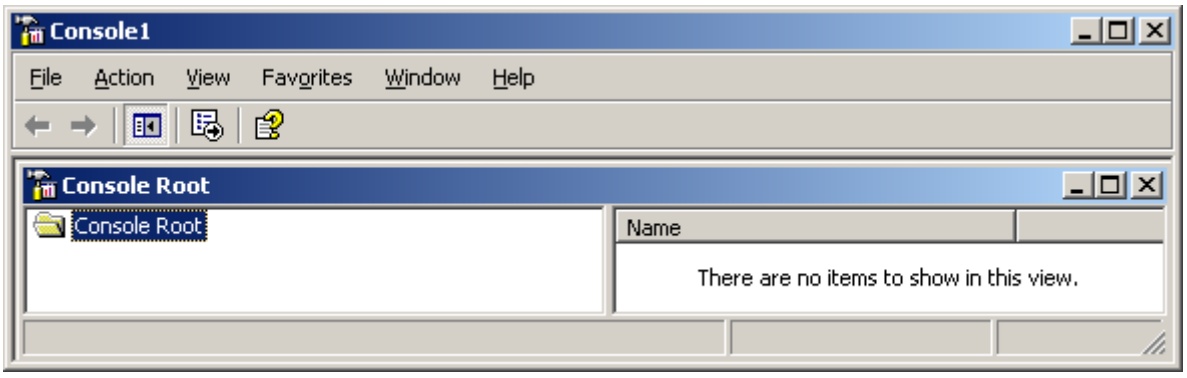
۲۸-۲- کار با MMC

برای حل اولین مشکل، مایکروسافت این راه حل را در نظر گرفته است: می توان یک Console جدید تعریف نمود و سپس تمامی کنسول های مدیریتی مورد نظر را به آن اضافه نمود. حال با باز کردن این Console، تمامی کنسول های مدیریتی خود را به صورت مجتمع و یکجا مشاهده خواهید نمود.

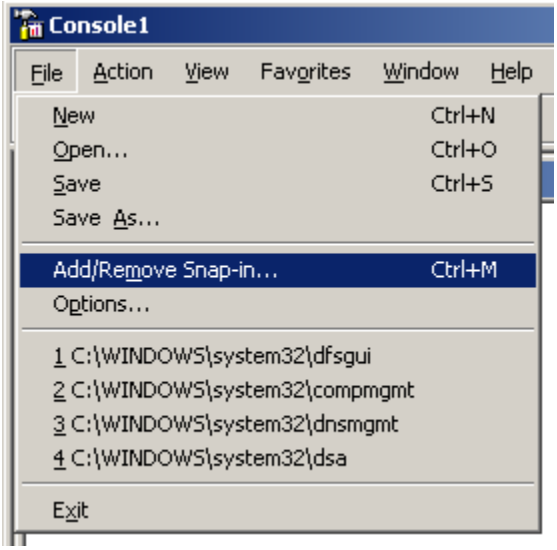
برای ساخت یک Console جدید، ابتدا وارد Run شده و سپس دستور mmc را وارد نمایید.



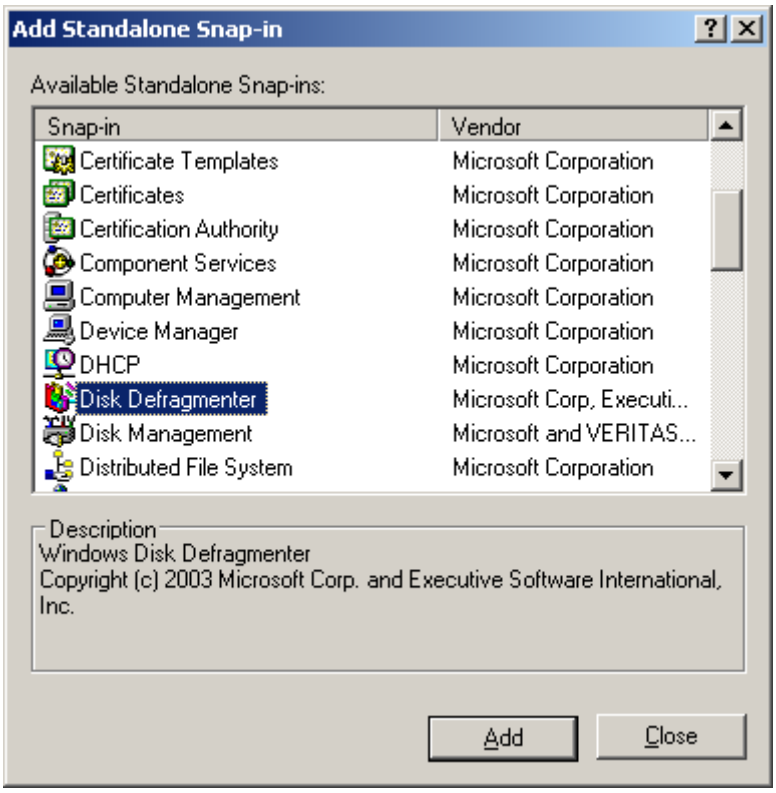
با این کار، یک Console جدید باز می شود.



حال نوبت به اضافه کردن کنسول های مدیریتی خود به این Console می شود (مانند DHCP و DNS). بدین منظور از منوی File، گزینه Add/Remove Snap-in را انتخاب کنید.

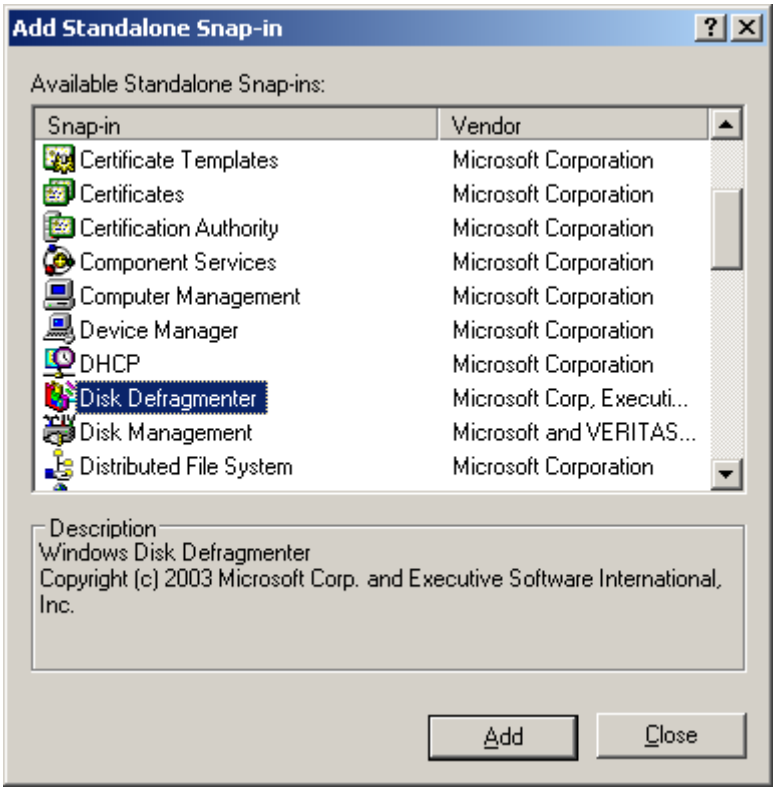


سپس در صفحه باز شده، کنسول های مدیریتی خود را انتخاب کرده و روی دکمه Add کلیک کنید.

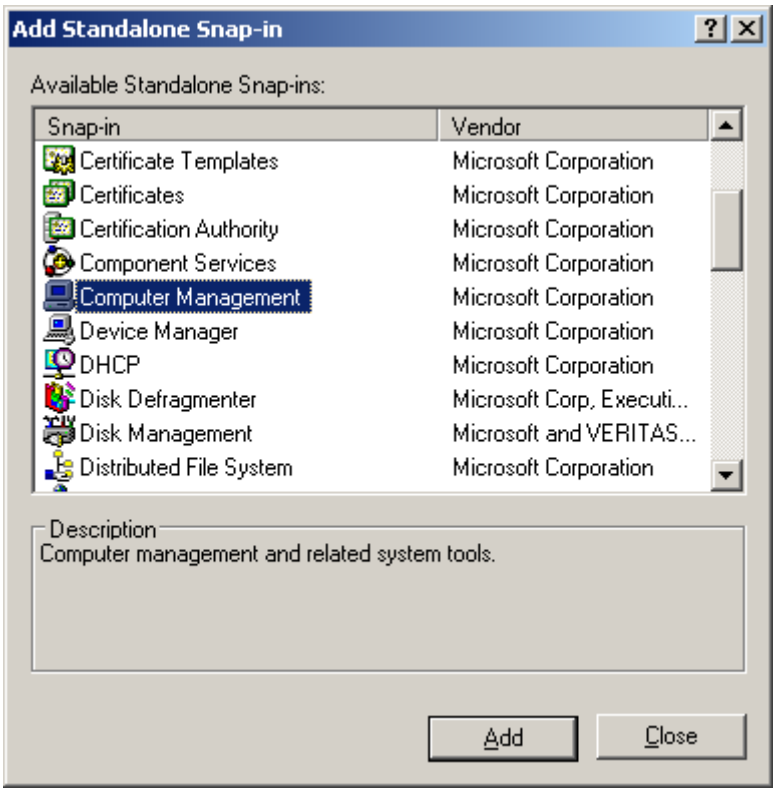


تا اینجا، ما برای مشکل اول و دوم راه حلی پیدا کرده ایم. اما مشکل سوم، یعنی کنسول های مدیریتی کامپیوتر های راه دور هنوز به قوت خود باقی است. برای حل این مشکل نیز از این روش استفاده می شود: هنگام انتخاب کرده یک کنسول مدیریتی، سیستم از ما سوال می پرسد که آیا می خواهید این کنسول مدیریتی، تنظیمات همین کامپیوتر را نشان دهد یا اینکه اطلاعات یک کامپیوتر راه دور را به نمایش در آورد؟ با انتخاب یک کامپیوتر راه دور، مشکل سوم نیز برطرف می شود. توجه نمایید که برای کنترل مدیریتی یک کامپیوتر راه دور، نیازی به نام کاربری و رمز عبور نیست. البته توجه داشته باشید که نمی توان به همه کنسول های مدیریتی راه دور دسترسی داشت و هنگام انتخاب آن های که قابلیت مدیریت از راه دور ندارند، سیستم از ما سوال نمی پرسد که آیا می خواهید این کنسول مدیریتی محلی باشد یا راه دور؟ و خودش آن را به صورت محلی انتخاب می کند.

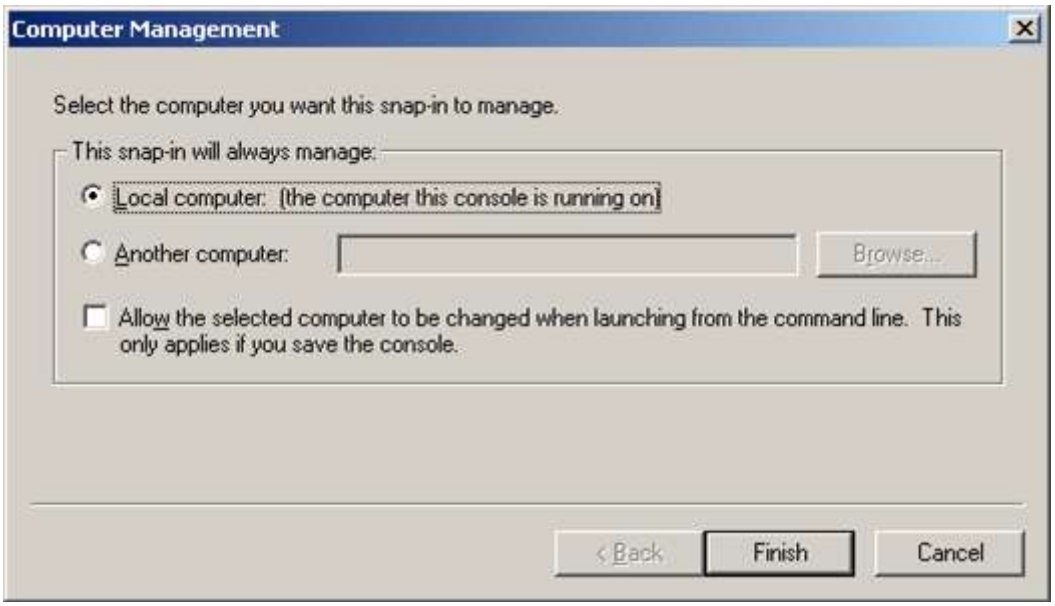
فرض کنید که می خواهیم کنسول مدیریتی Disk Defragment را اضافه کنیم؛ بدین منظور آن را انتخاب کرده و روی Add کلیک کنید. کنسول مدیریتی Disk Defragment، فقط قابلیت مدیریت به صورت محلی را دارد. لذا سیستم از ما سوالی در مورد محلی یا راه دور بودن آن نمی پرسد.



حال فرض کنید که می خواهیم کنسول مدیریتی Computer Management را اضافه کنیم. این کنسول مدیریتی قابلیت اتصال به صورت محلی و راه دور را دارد. لذا هنگام Add کردن آن، سیستم سوالی در مورد محلی یا راه دور بودن آن خواهد پرسید.

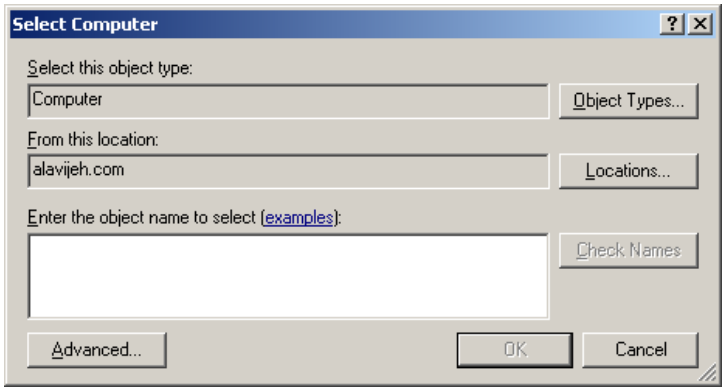


اگر می خواهید که این کنسول مدیریتی، فقط کامپیوتر خود شما را کنترل کند، گزینه Local computer را انتخاب کرده و سپس روی Finish کلیک کنید.

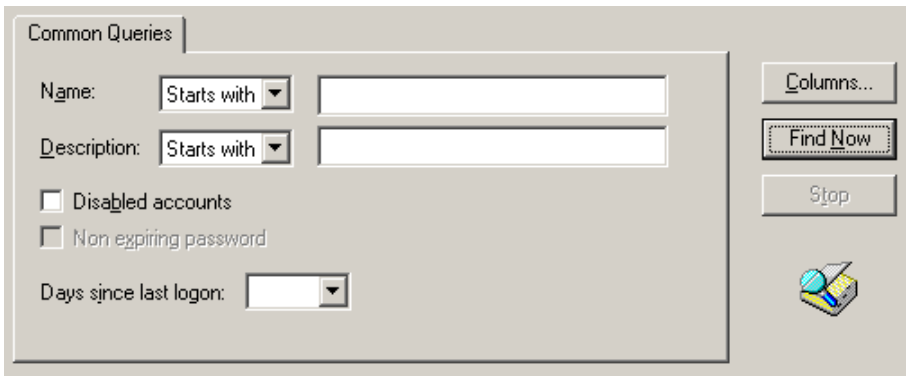


اما اگر می خواهید به کنسول مدیریتی کامپیوتر راه دور متصل شوید، گزینه Another computer را انتخاب کنید. حال دو راه پیش رو دارید. اول اینکه آدرس کامپیوتر را به صورت متنی در جعبه متن زیر وارد نمایید. دوم اینکه کامپیوتر راه دور را به صورت Visual انتخاب کنید. بدین منظور روی دکمه Browse کلیک کنید.

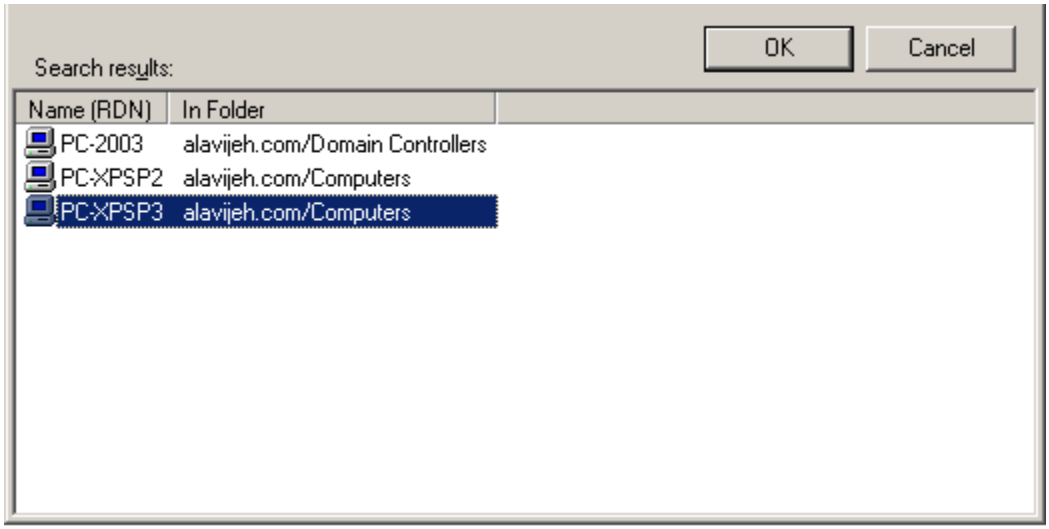
در صفحه باز شده، روی دکمه Advanced کلیک کنید.



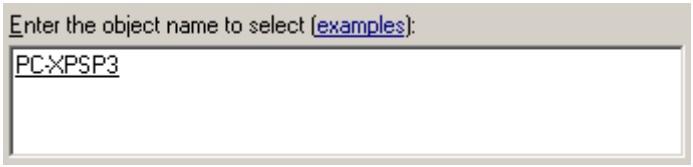
سپس در صفحه باز شده، برای پیدا کردن کامپیوتر های موجود در شبکه، روی دکمه Find Now کلیک کنید.



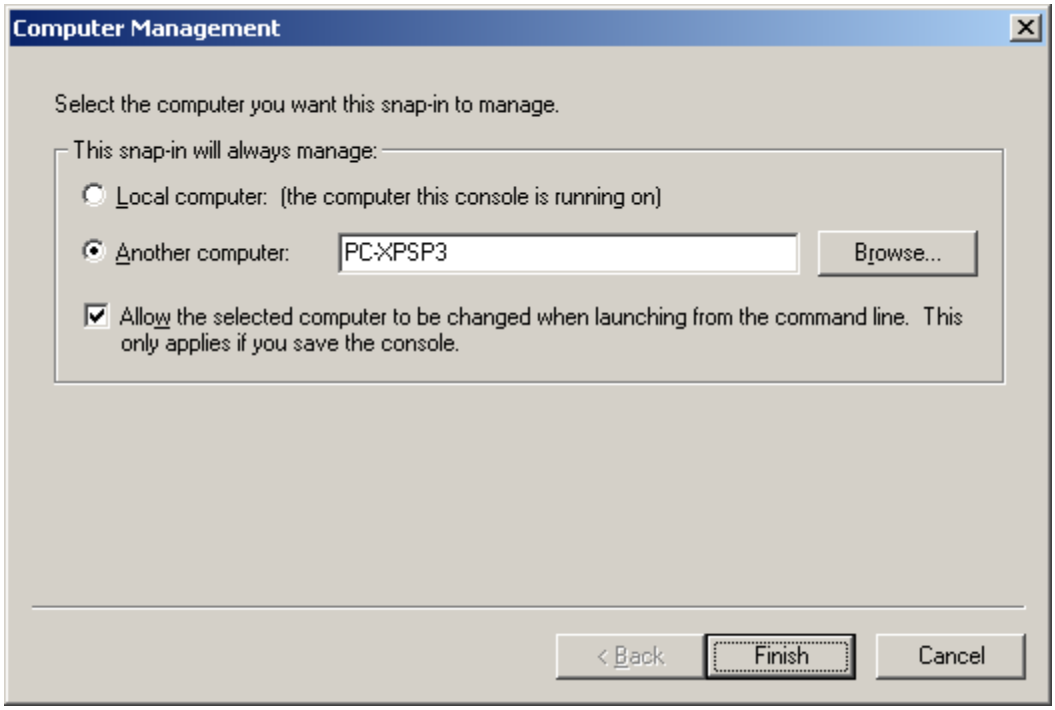
سپس کامپیوتر راه دور مورد نظر را انتخاب کرده و روی OK کلیک کنید.



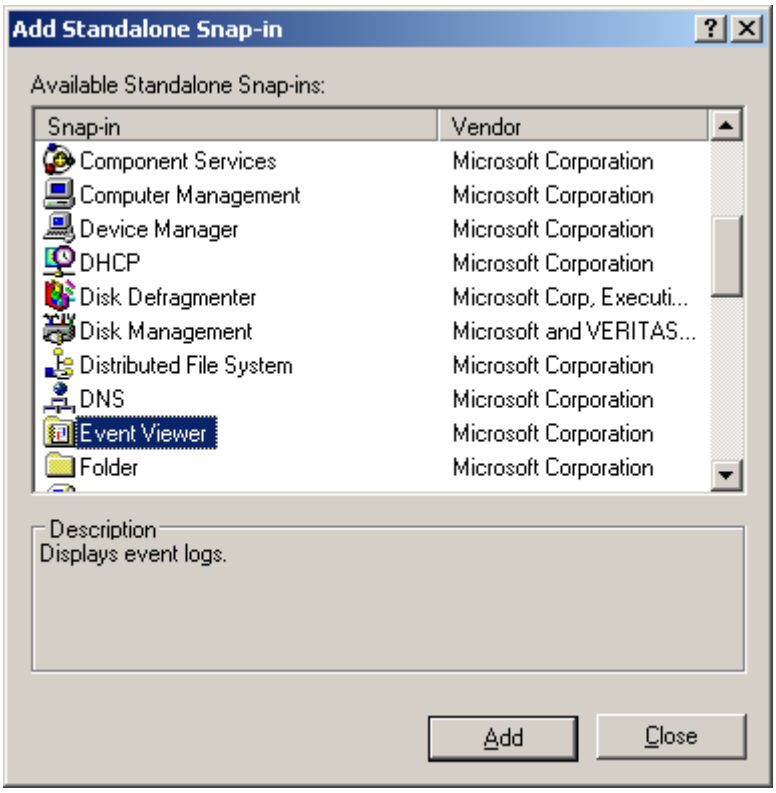
با این کار بایستی نام کامل (FQDN) کامپیوتر راه دور را مشاهده نمایید.



با انتخاب کامپیوتر راه دور، بایستی شکلی مانند زیر نمایان شود. حال روی Finish کلیک کنید.

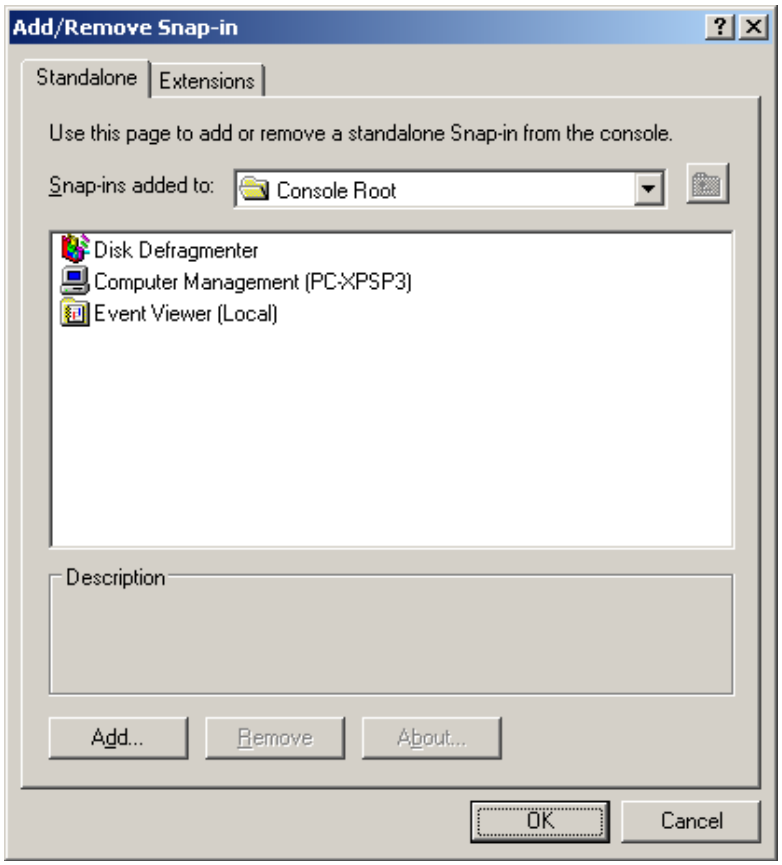


به عنوان کنسول مدیریتی آخر، فرض کنید که قصد داریم کنسول Event Viewer کامپیوتر خود را (نه کامپیوتر راه دور را) به کنسول های خود اضافه کنیم. بدین منظور، پس از انتخاب Event Viewer، روی دکمه Add کلیک کنید.

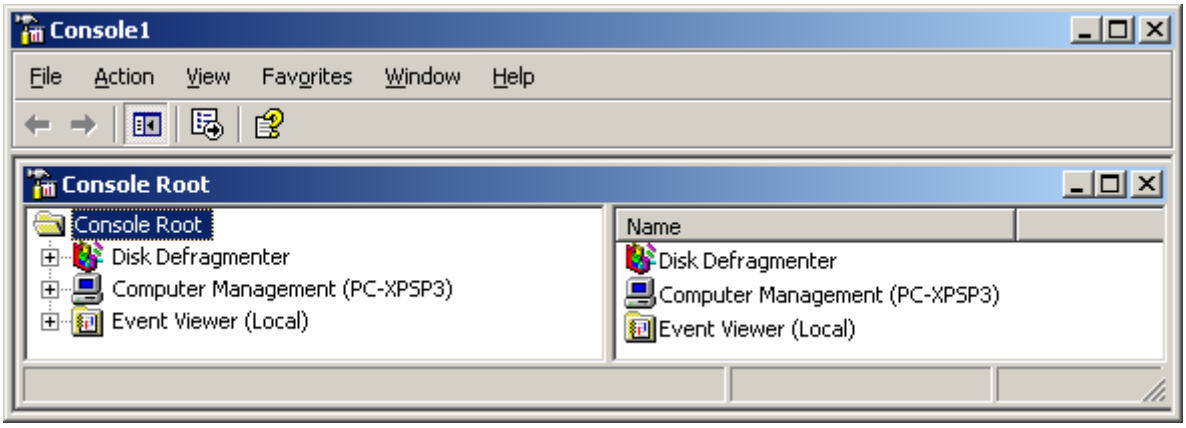


سپس در صفحه باز شده، گزینه Local computer را انتخاب کرده و روی Finish کلیک کنید.

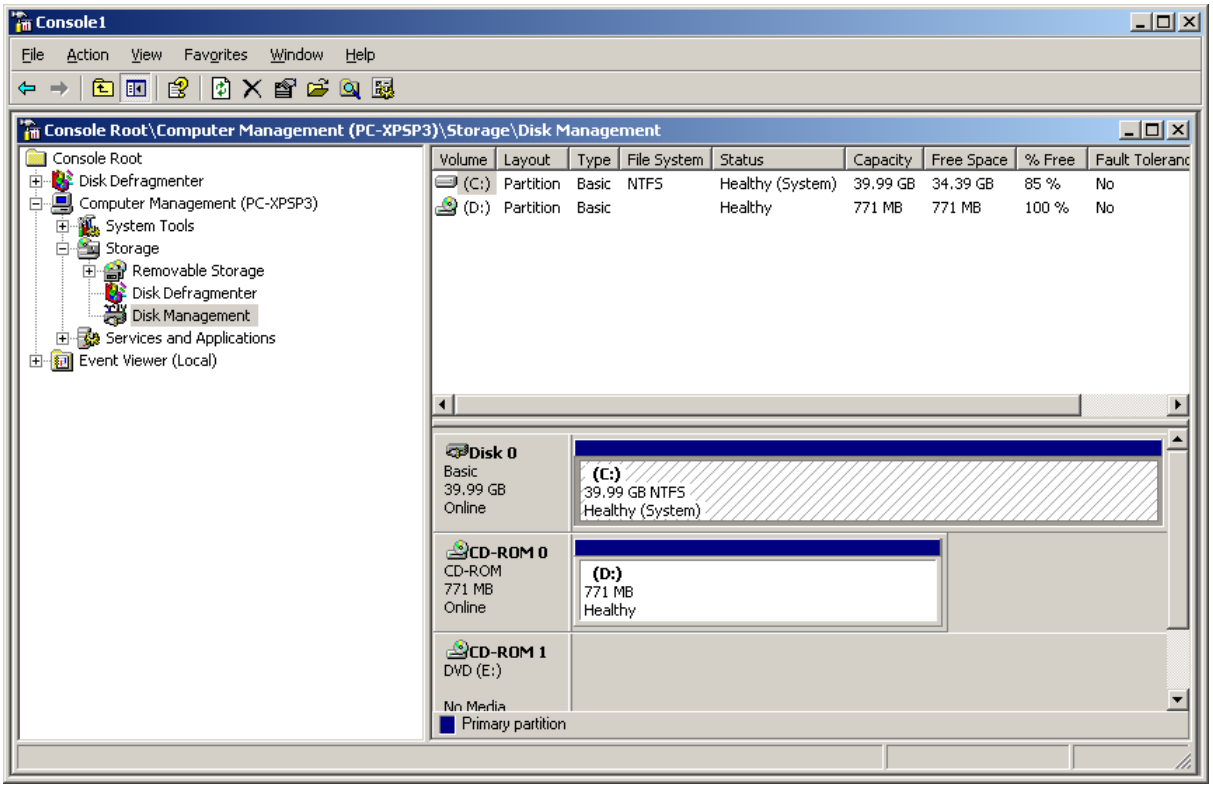
در نهایت روی Close کلیک کنید. بدین ترتیب هر ۳ کنسول مدیریتی انتخاب شده را مشاهده خواهید نمود.



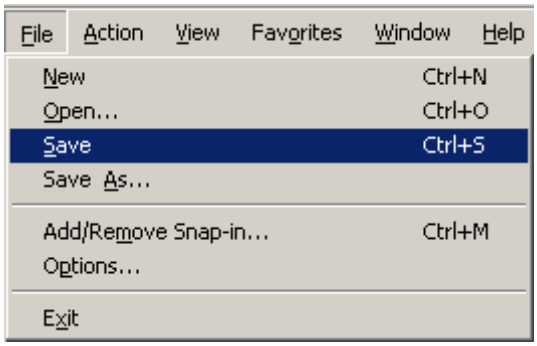
در نهایت روی OK کلیک کنید. بدین ترتیب هر ۳ کنسول مدیریتی شما، در یک کنسول واحد به نمایش در خواهد آمد.



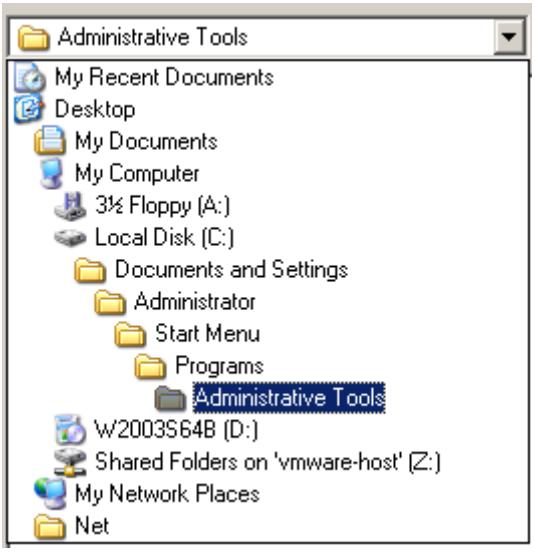
حال برای مدیریت هر کدام از کنسول ها، تنها کافیست آن را انتخاب نمایید. در این مثال، ما کنسول مدیریتی Computer Management که به صورت راه دور است را تنظیم خواهیم نمود تا بدین وسیله متوجه شوید که برای تنظیم یک کنسول مدیریتی راه دور نیازی به نام کاربری و رمز عبور نمی باشد.



حال بایستی این کنسول مدیریتی ساخته شده جدید را ذخیره نمایید تا دیگر نیازی به انجام موارد فوق نداشته باشید. بدین منظور از منوی File گزینه Save را انتخاب نمایید.

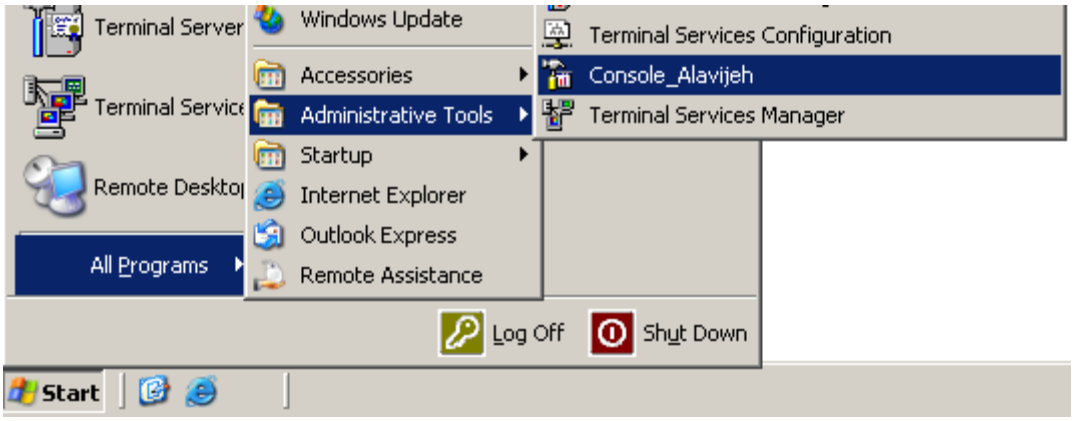


سپس آن را در همان مسیر پیش فرض، یعنی در پوشه Administrative Tools ذخیره کنید. به شکل زیر دقت نمایید.

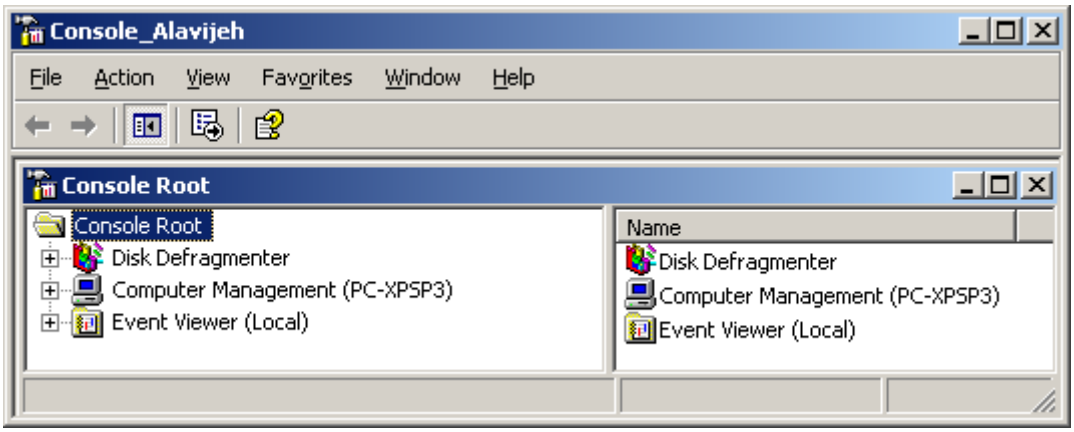


سپس نامی نیز برای این کنسول جدید وارد نمایید.

حال برای دسترسی به این کنسول مدیریتی می توانید به مسیر Administrative Tools ➔ All Programs ➔ Start رفته و کنسول ساخته شده را باز نمایید. توجه فرمایید که این مسیر با مسیر Administrative Tools ➔ Start که تاکنون کارهای مدیریتی خود را از آن انتخاب می کردیم، متفاوت است.



با بازکردن کنسول مدیریتی ساخته شده، کنسول های خود را به صورت مجتمع مشاهده خواهید نمود.



فصل ۲۹

Distributed File System یا DFS

۲۹-۱- متمرکز کردن اطلاعات Share شده

در فصل ۹، شما با راه اندازی شبکه های Workgroup و همچنین به اشتراک گذاری فایل ها و پوشه ها آشنا شدید. موضوعی که اکنون مطرح می شود این است که فرض کنید هر کدام از کامپیوتر ها نرم افزار خاصی را برای استفاده دیگران به اشتراک گذاشته اند. حال شما به یک نرم افزار نیاز پیدا می کنید؛ و فرض می کنیم که این نرم افزار در شبکه به اشتراک گذاشته شده باشد. تنها راه دسترسی به آن این است، که به تمام کامپیوتر های شبکه، تک تک Login کرده، و در فایل های اشتراک گذاشته شده آن ها، به جستجوی برنامه مورد نظر بپردازیم. علاوه بر این مشکل، مشکل دیگری نیز وجود دارد که ما بایستی به ازاء تک تک کامپیوتر ها، یک نام کاربری و رمز عبور ثبت شده در آن کامپیوتر را داشته باشیم. برای حل این مشکلات مایکروسافت Distributed File System یا به اختصار DFS را معرفی کرد.

۲۹-۲- Distributed File System چیست؟

همانگونه که اطلاع دارید، File System مکانیزمی برای نگهداری **اطلاعات و مشخصات** فایل های موجود در یک سیستم می باشد. هر سیستم یک File System مخصوص خود را دارد و لذا به آن Local File System می گویند. در مقابل Local File System، Distributed File System قرار دارد. یعنی اینکه یک کامپیوتر این قابلیت را پیدا می کند که **اطلاعات و مشخصات** فایل های موجود بر روی دیگر کامپیوتر ها را نگهداری می کند. حال برگردیم به بحث قبلی. در بالا ما دو مشکل: جستجوی تمامی کامپیوتر های شبکه و نیز نیاز به دانستن رمز های عبور هر کامپیوتر را مطرح کردیم و گفتیم که برای حل آن Distributed File System یا به اختصار DFS عرضه شد. روند کار برای حل این مشکل بدین صورت است که هر کامپیوتری که قصد به اشتراک گذاری فایلی را داشته باشد، آن را به یک کامپیوتر خاص معرفی می کند (فایل را در آن کپی نمی کند، بلکه فقط یک Link به آن فایل می دهد). این کامپیوتر خاص بهتر است کنترل کننده دامنه باشد (DC). لذا **لینک** تمامی فایل های Share شده، در یک نقطه متمرکز می گردند. حال اگر فردی به یک فایل نیاز پیدا کرد، با نام کاربری و رمز عبور خود که در سرور ذخیره شده است، به سرور متصل شده و فایل مورد نظر را در آن جستجو می کند؛ و این یعنی نیاز به **یک** نام کاربری و رمز عبور و نیاز به **یکبار** جستجو.

۲۹-۲-۱- مراحل انجام کار DFS

۱. یک سرور را تبدیل به DFS Root Server کرده و روی آن یک پوشه Root درست می کنیم.
۲. هر پوشه Share شده ی مهمی که داخل ساختار شبکه هست را پیدا کرده و آدرس آن پوشه را به DFS Server مان اضافه می کنیم.
۳. حالا هر کاربری که می خواهد از فایلهای Share شده ی پخش شده در شبکه ما استفاده کند، می رود سراغ DFS Server که خودش یک پوشه Root دارد که داخل این پوشه، Shortcut فایل های اضافه شده توسط کاربران، قرار گرفته است.
۴. با کلیک بر روی پوشه مورد نظر، کاربر به سمت کامپیوتری که پوشه مورد نظر روی آن قرار دارد، ارجاع داده می شود.

پس مشخص شد که کار اصلی DFS این است که: یک لیست بزرگ از فایل هایی که کاربران ممکن است به آن ها نیاز داشته باشند را از روی شبکه جمع کرده و توی یک پوشه نگهداری می کند تا کاربران به جای اینکه مجبور شوند هر کامپیوتر را برای وجود پوشه Shareشده خاص جستجو کنند، بتوانند با یک بار وصل شدن به پوشه ریشه، کل محتوای Share شده ی شبکه را ببینند.

۲۹-۲-۲- انواع DFS

DFS به دو نوع اصلی تقسیم می شود:

۱. Stand-Alone DFS Root

در این حالت، ما Active Directory نداریم و بر روی یک سیستم عامل سرور اقدام به اجرا کردن سرویس DFS می کنیم. در این حالت، فایل های مورد نظر ما Replicate نمی شوند و اگر DFS Server مان Down شود، کاربران قادر به دسترسی به پوشه های Shareشده نخواهند بود. در ضمن برای Fault Tolerance هم مجبوریم که از ساختارهای Clustering خود سیستم عامل استفاده کنیم.

۲. Domain DFS Root

در این یکی حالت، ما DFS را روی یک ساختار Domain Model نصب می کنیم، Replication بین Root های مختلف به کمک ساختاری به نام FRS انجام شده و Fault Tolerance هم توسط FRS یا File Replication Service صورت می گیرد.

در حالت اول اگه سرور Down شود، کاربران قادر به دسترسی به پوشه های Shareشده نخواهند بود. برای اینکه این اتفاق نیفتد، می توانید اقدام به استفاده از قابلیت Network Load Balancing ویندوز برای کلاستر کردن سیستم هایتان کنید و سپس روی چندین سرور یک Root Folder یکسان تعریف نمایید که همگی به مکان های معینی اشاره می کنند. در این حالت، اگر سروری Down شود، کاربران به سرور بعدی هدایت شده و چون Root Folder سرور ها یکسان است، پس کاربران متوجه تغییری نخواهند شد. اما یکی از مشکلات این حالت این است که اگر تغییری در یکی از Root Folder های یکی از سرور ها بدهیم، باید سریع برویم سراغ سرور های دیگر عضو کلاستر و آن ها را نیز تغییر بدهیم.

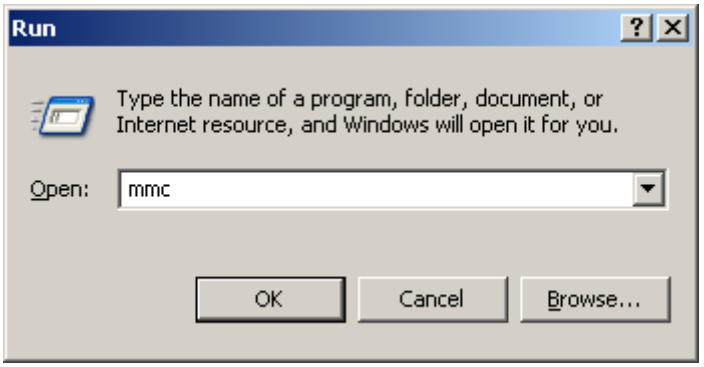
در حالت دوم، یک سرور عضو Active Directory، مسئول کنترل Root Folder ها می شود. اگر بخواهید اقدام به Fault Tolerance کنید، نیازی به Clustering ویندوز نیست، چرا که ساختاری به نام File Replication Service خودش اقدام به Replicate کردن فایل های هر سرور با دیگر سرورهای DFS کرده و بدین ترتیب اگر چندین سرور DFS داشته باشید، اطلاعات این ها هر چند دقیقه با هم Replicate شده و هر تغییری که اولی کرده باشد، در بقیه نیز اعمال می کند.

ما در ادامه، حالت دوم را توضیح می دهیم.

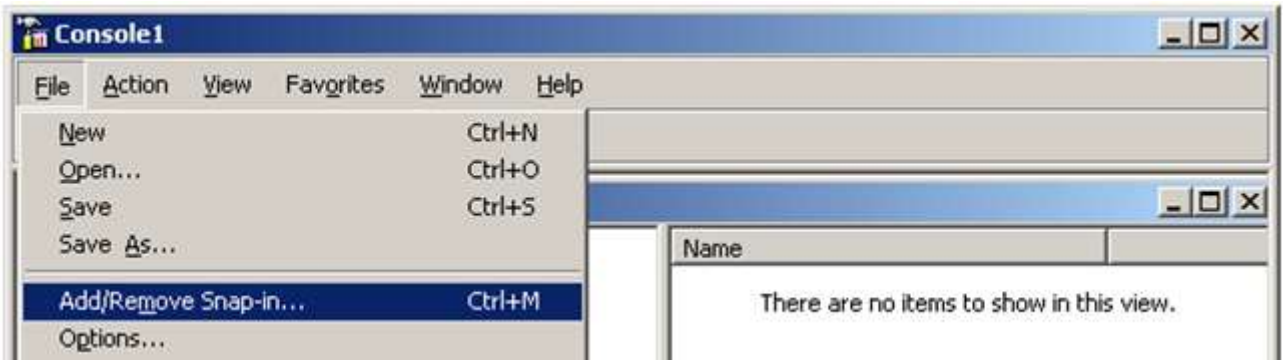
۲۹-۳- Distributed File System در ویندوز سرور

اینک به آموزش راه اندازی DFS می پردازیم. اول از همه یادتان باشد که هم پورت ۴۴۵ باید برای DFS باز باشد و هم اینکه DFS یک سرویس به نام Distributed File System دارد که بایستی آن را فعال نمایید. سپس محیط Distributed File System را باز نمایید. بدین منظور از مسیر Administrative Tools ➔ Start گزینه Distributed File System را انتخاب نمایید:

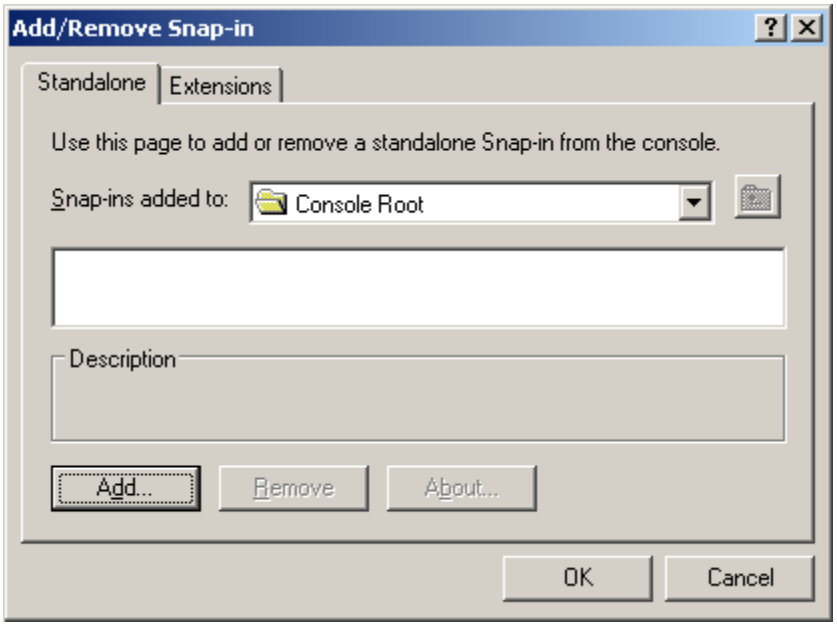
اگر Distributed File System را در این مسیر نیافتید، ابتدا وارد Run شده و عبارت mmc را وارد نمایید تا کنسول مدیریتی مایکروسافت نمایان شود.



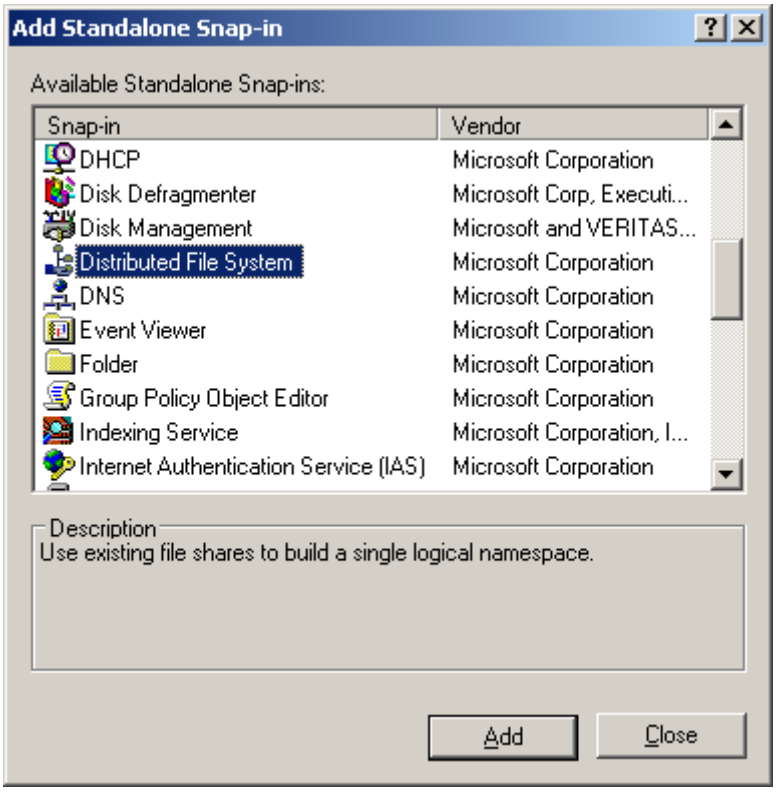
با این کار، صفحه mmc را مشاهده می نمایید. در مورد mmc، فصل گذشته صحبت کردیم. حال نوبت به بازکردن کنسول DFS می شود. برای این کار، از منوی File گزینه Add/Remove Snap-in را انتخاب کنید.



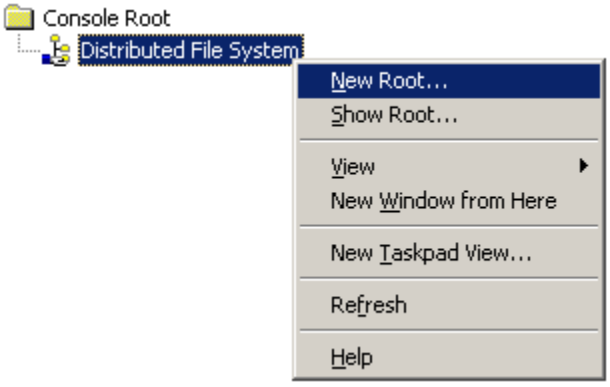
حال نوبت به انتخاب کنسول DFS می شود. لذا در صفحه باز شده، روی دکمه Add کلیک کنید.



حال در این صفحه، Distributed File System را انتخاب کرده و روی Add کلیک کنید.

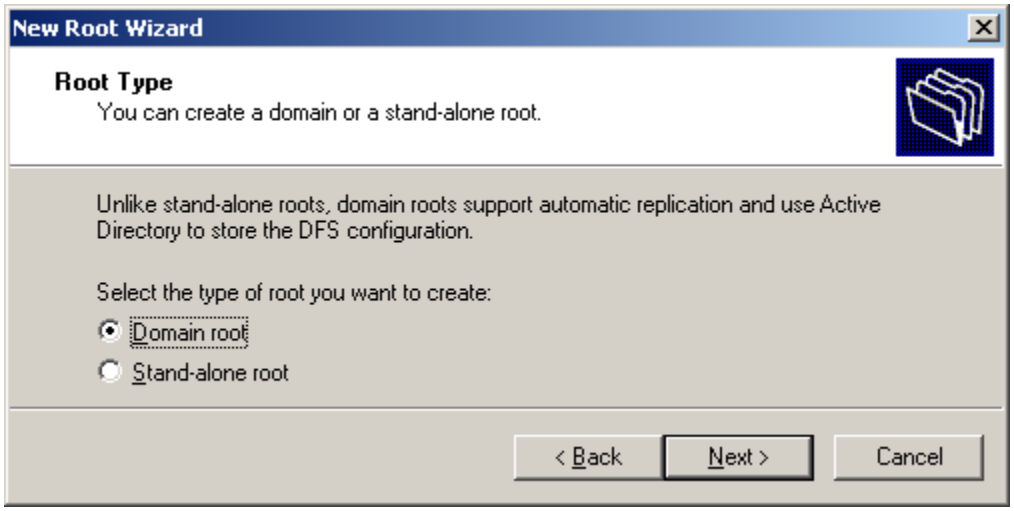


در مرحله بعد، شما بایستی بر روی سرور فضایی را برای ذخیره **اطلاعات و مشخصات** مربوط به فایل های Share شده تعیین نمایید. توجه نمایید که فایل ها از روی Client بر روی Server کپی نمی شوند؛ بلکه در سرور، فقط Linkی به آن فایل ها می دهیم. بدین منظور بر روی Distributed File System راست کلیک کرده و سپس گزینه New Root را انتخاب کنید. در اینجا Root اشاره به نقطه شروعی (یک آدرس) دارد که برای دسترسی به فایل ها و پوشه های Share شده از آن استفاده می کنیم. مثلاً ریشه (Root) درایو C:\، محلی آغازین برای دسترسی به فایل ها و پوشه های موجود در این درایو است.

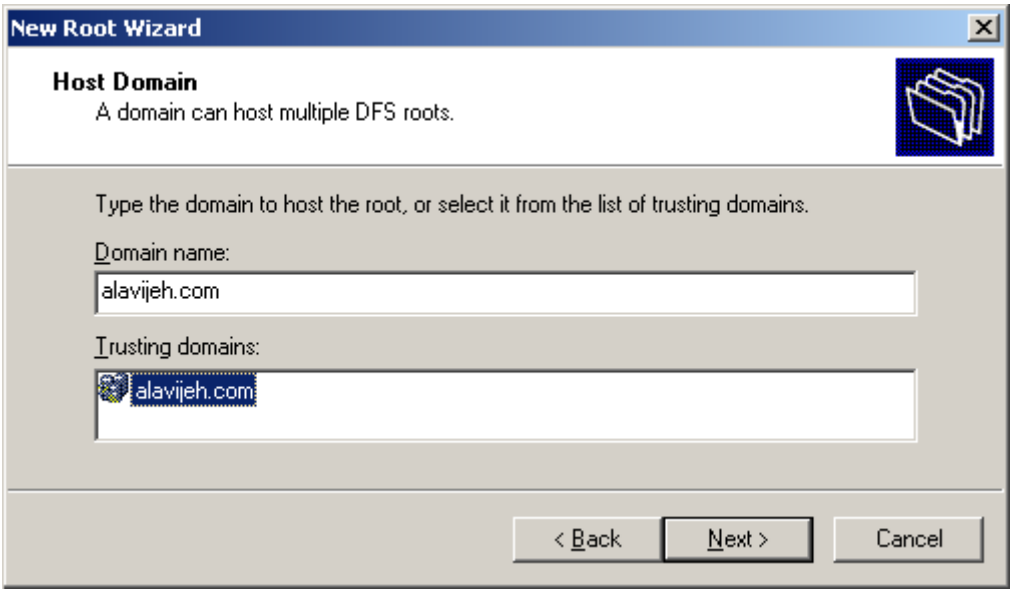


در صفحه خوش آمدگویی، Next را بزنید.

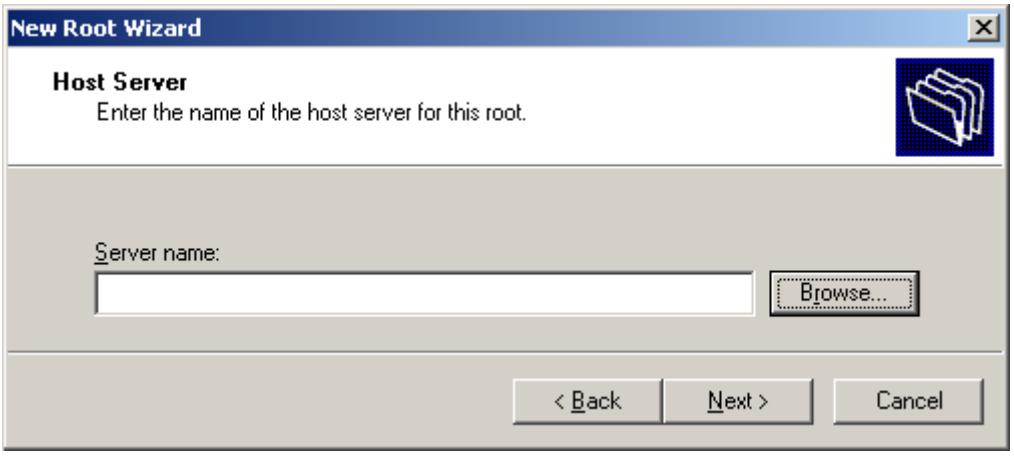
در مرحله بعد تعیین نمایید که کامپیوتری که می خواهد این فضا را نگهداری کند (فضای متمرکز برای اشاره به فایل های Share شده)، آیا در یک Domain قرار دارد یا اینکه یک کامپیوتر مستقل (Stand-alone) است؟ از آنجایی که ما Domain را راه اندازی کرده و کامپیوتر ما در Domain قرار دارد، لذا ما گزینه Domain root را انتخاب می کنیم.



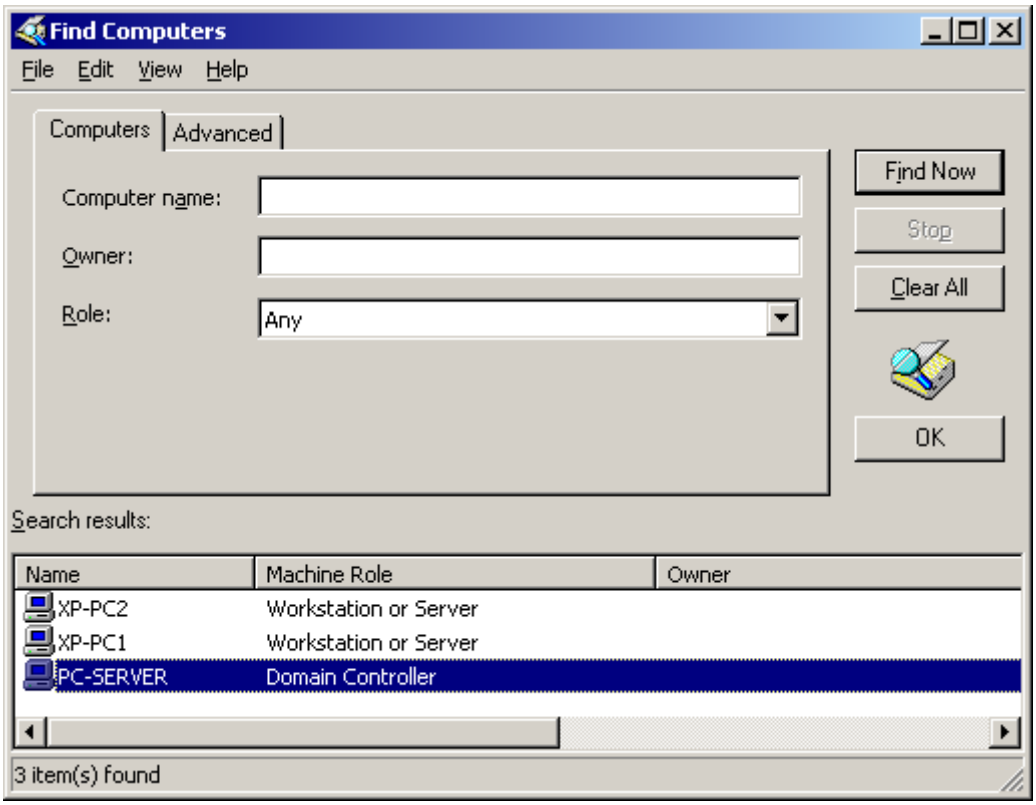
در این صفحه دامنه ای که کامپیوتر در آن قرار دارد را انتخاب نمایید. توجه نمایید که این دامنه می تواند یک دامنه Trust (مورد اعتماد) باشد.



در مرحله بعد کامپیوتری که فضا را نگهداری خواهد کرد تعیین نمایید. توجه نمایید که این کامپیوتر می تواند سرور نباشد. ولی حتما بایستی جزء دامنه باشد. در اصل، این همان سروری می باشد که اقدام به ذخیره ی اطلاعات Root Folder می کند. برای انتخاب کامپیوتر، روی Browse کلیک کنید.

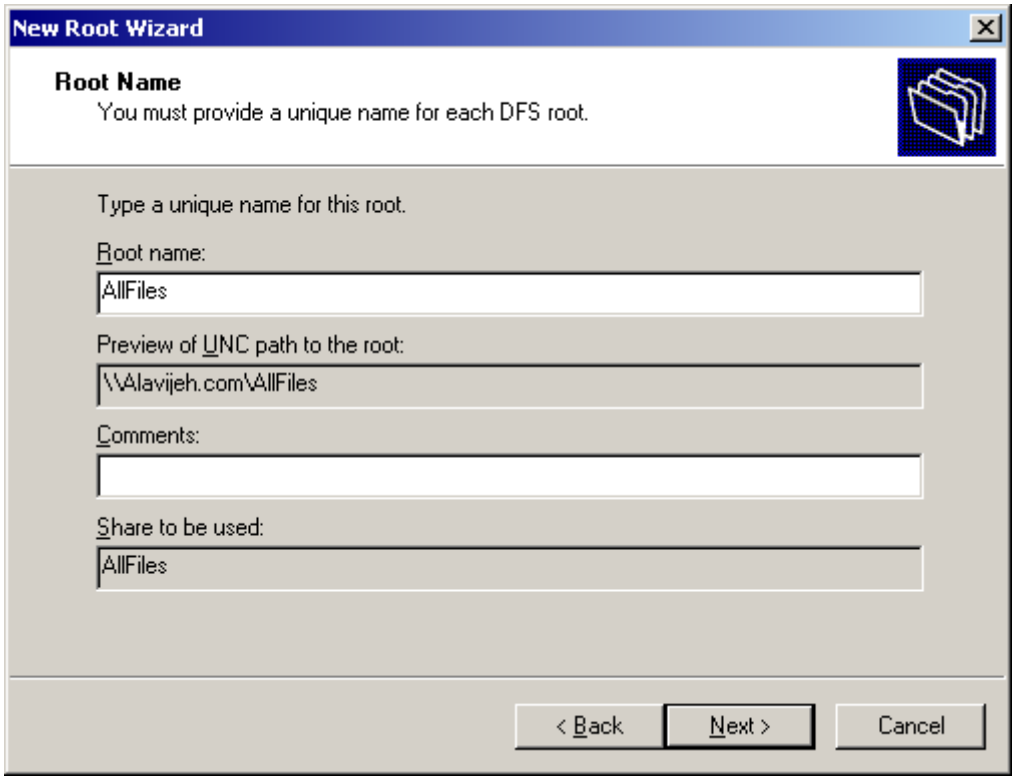


در صفحه باز شده، کامپیوتر مورد نظر را انتخاب کرده و روی OK کلیک کنید.



از آنجایی که این کامپیوتر در دامنه قرار دارد، پس از انتخاب آن، نام کامل آن (FQDN) نمایان می شـود. یـادآوری: FQDN، همان نام کامپیوتر به همراه نام دامنه آن می باشد.

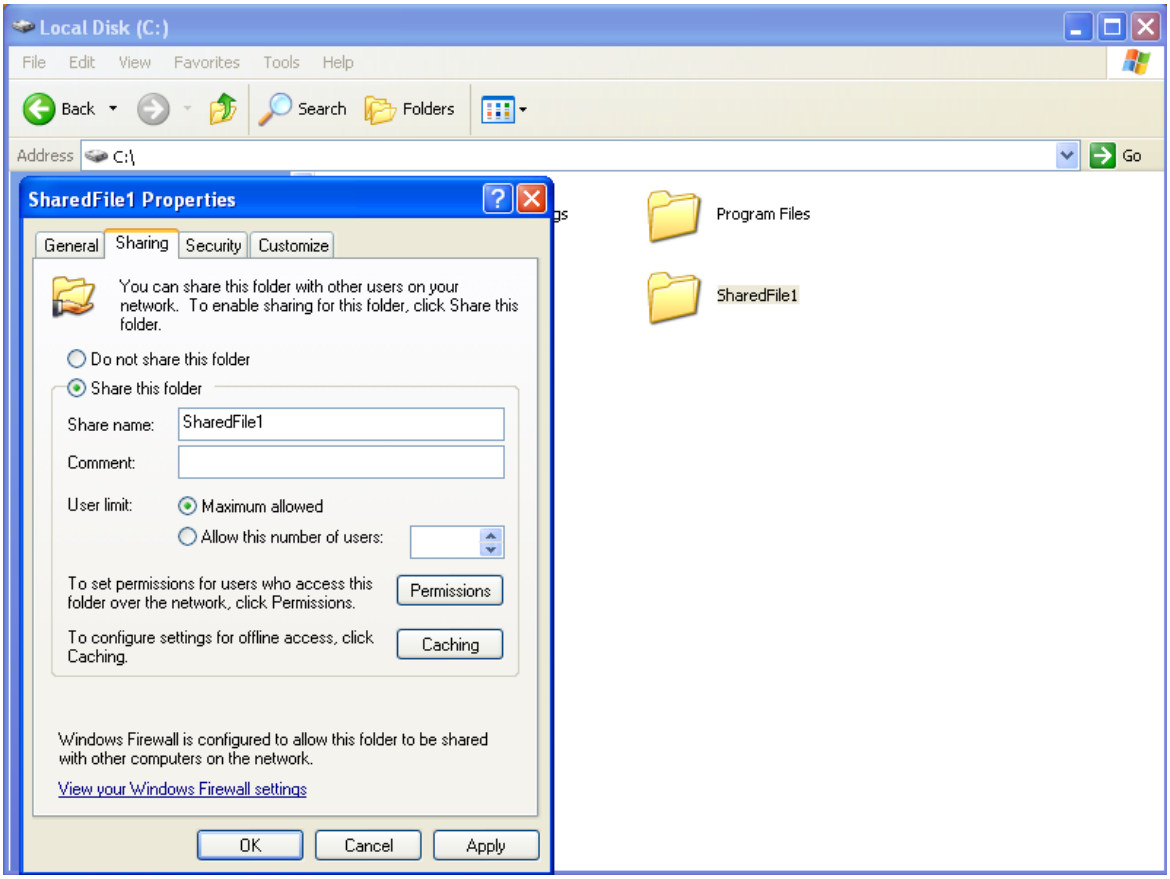
در مرحله بعد، نام یک پوشه Share شده در کامپیوتری که Root ها را نگهداری می کند وارد نمایید. کاربرد این نام، این است که کاربران پس از Login به سرور، با ورود به پوشه ای به همین اسم، می توانند فایل های Share شده در شبکه (که به سرور معرفی شده اند) را مشاهده نمایند. در این مثال ما نام را AllFiles در نظر گرفته ایم. این بدان معنا است که در سـرور Root DFS، پوشه ای به نام AllFiles، به اشتراک گذاشته شده است. لذا کاربران برای مشاهده فایل های Share شـده بایسـتی بـه مسیر \\alavijeh.com\AllFiles مراجعه نمایند. تا این لحظه بایستی متوجه شده باشید که می توان **اطلاعات و مشخصـات** فایل های Share شده را در هر کامپیوتری ذخیره نمود، اما دسترسی به آن ها، تنها به کمک اتصال به سرور (DC) انجام مـی گیرد. باز هم تاکید می کنم که **در این صفحه، نام یکی از پوشه های Share شده را وارد نمایید**. اطلاعـات Shortcutهـا در این پوشه ذخیره خواهد شد.



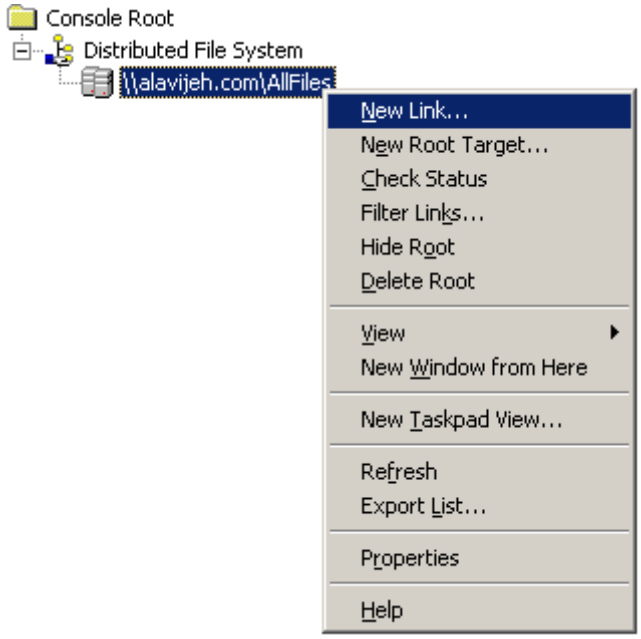
در نهایت، روی Finish کلیک کنید.

۲۹-۴- ایجاد Link به یک پوشه Share شده

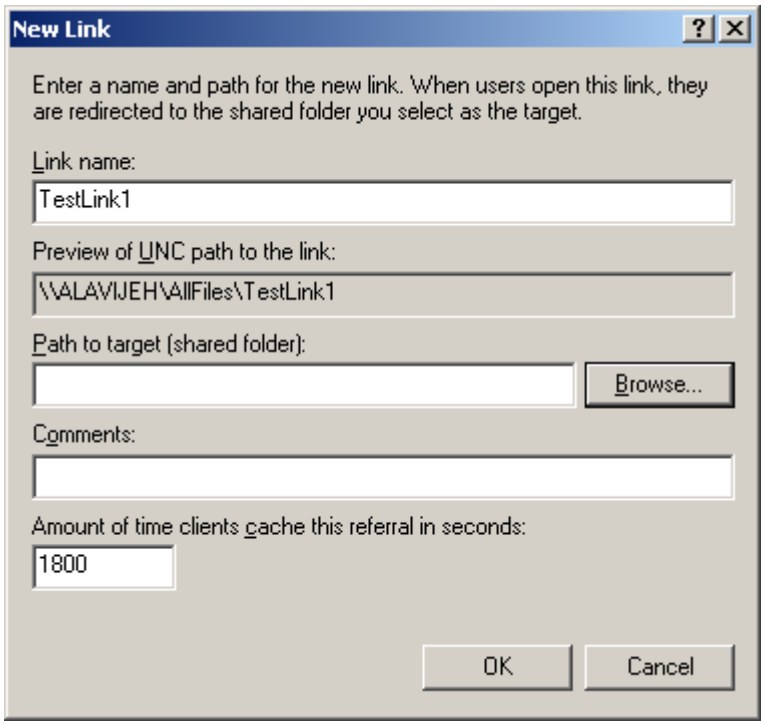
حال بایستی در Client فایلی را Share کنید. در این مثال ما پوشه C:\SharedFile1 را در Client به اشتراک گذاشته ایم.



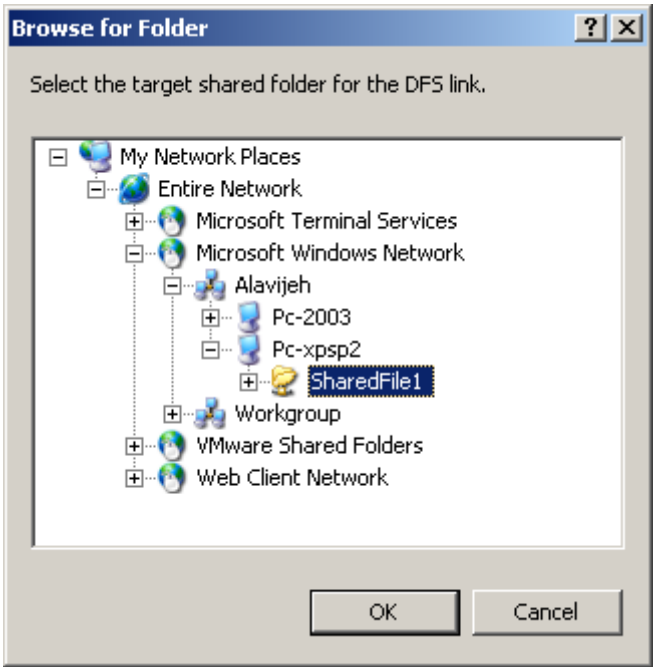
حال مجددا به سرور بر گردید. در این مرحله، برای اینکه این پوشه توسط دیگر کامپیوتر ها قابل مشاهده باشد، بایستی یک Link به آن پوشه ایجاد کنیم. بدین منظور روی Root ساخته شده در سرور راست کلیک کرده و گزینه New Link را انتخاب کنید.



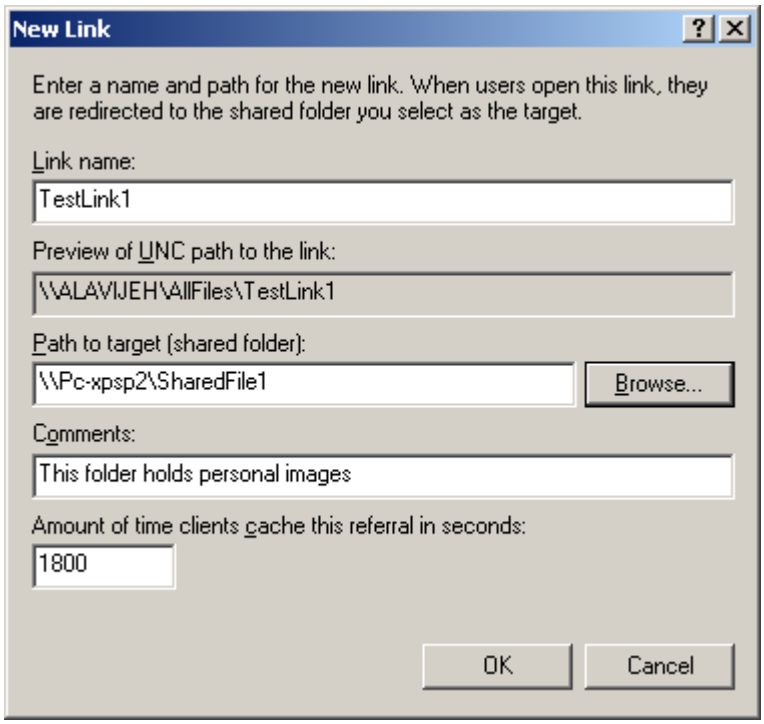
در صفحه باز شده، در قسمت Link Name، یک نام دلخواه برای Link ایجاد شده وارد نمایید به طوری که معرف محتویات آن باشد. سپس در قسمت Path to target، مسیر فایل Share شده را وارد نمایید. بدین منظور روی دکمه Browse کلیک نمایید. توجه نمایید که مقدار موجود در جعبه متن Preview of UNC path to the link، مسیری را نشان می دهد که کاربران برای دسترسی به محتویات این پوشه Share شده بایستی طی نمایند.



در صفحه باز شده، ابتدا کامپیوتر مورد نظر و سپس پوشه Share شده آن را انتخاب نمایید. توجه نمایید که اطلاعات کامپیوتر های یک شبکه، در قسمت Microsoft Windows Network قرار دارد. به شکل توجه فرمایید.

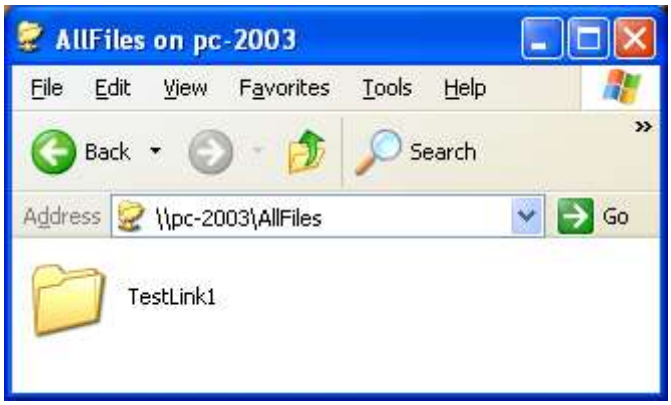


پس از انتخاب پوشه Share شده، شکلی مانند زیر را مشاهده می کنید. روی OK کلیک نمایید.



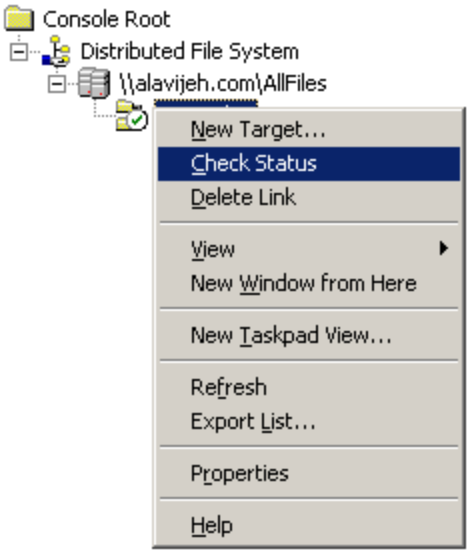
۲۹-۵- دسترسی به پوشه های Share شده

حال نوبت به استفاده از پوشه های Share شده می شود. بدین منظور مسیر Root ایجاد شده را در نوار آدرس یا در Run وارد نمایید. با این کار پوشه های Share شده و معرفی شده به سرور را مشاهده خواهید نمود.



برای تاکید می گویم که این صفحه، تمام پوشه های Share شده در شبکه را نشان نمی دهد. بلکه آن هایی را نشان می دهد که هم Share شده باشند و هم به سرور معرفی شده باشند (در سرور Linkی به آن ها ایجاد شده باشد).

همچنین در هر لحظه می توانید وضعیت یک Link را بررسی نمایید. بدین منظور روی Link ساخته شده راست کلیک کرده و گزینه Check Status را انتخاب نمایید.



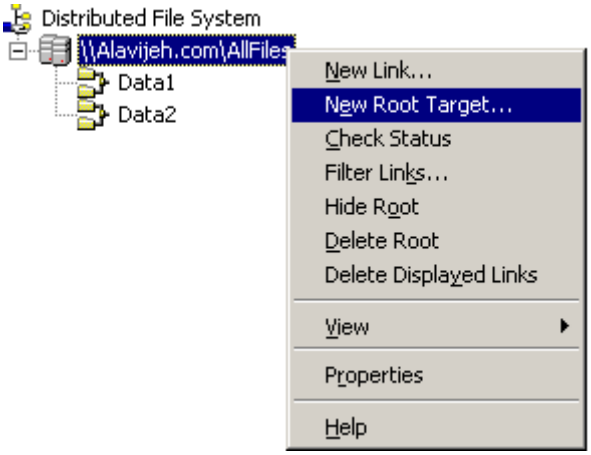
اگر کامپیوتری که این پوشه را Share کرده است، خاموش بوده یا در دسترس نباشد، روی آن Link، یک علامت × قرمز رنگ مشاهده خواهد شد. بدین معنا که دیگر کامپیوتر ها به این Link دسترسی نخواهند داشت.

۶-۲۹- Replication در DFS

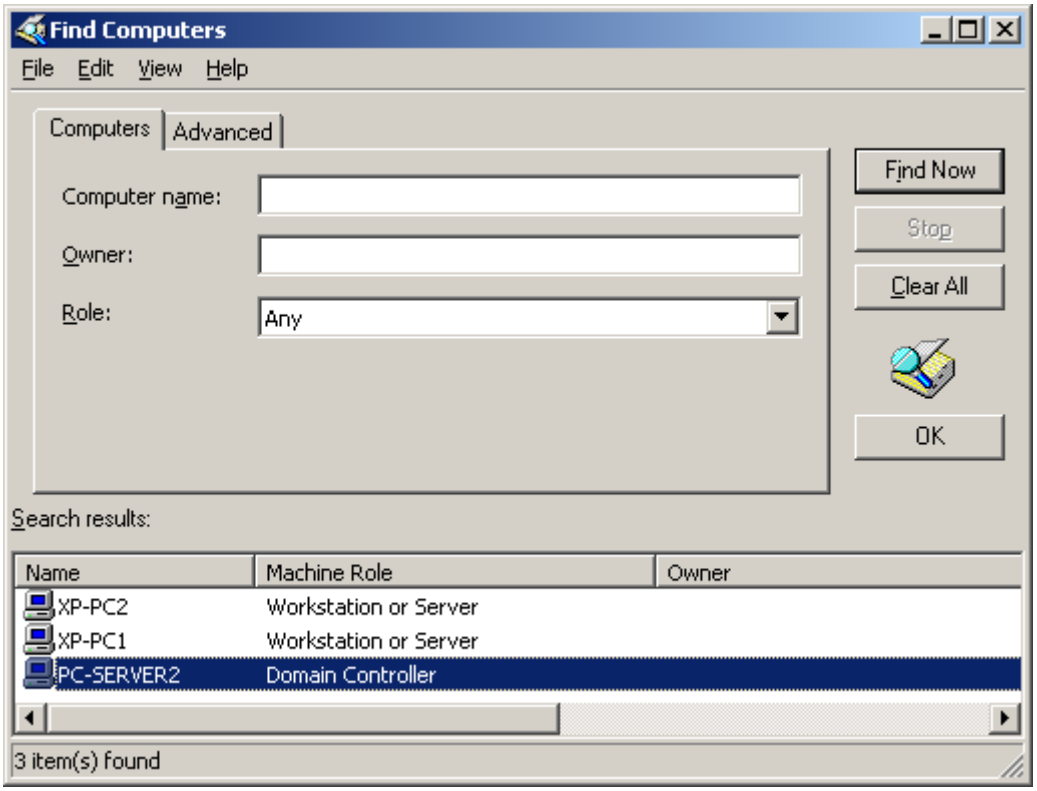
تنها بحثی که از DFS باقی می ماند، بحث FRS و Replication است. منظور از FRS و Replication، همان عملیات تکثیر Shortcut پوشه های Share شده در چندین سرور می باشد، به طوری که با خراب شدن یک سرور DFS، سرور دیگر بتواند عملیات سرویس دهی را انجام دهد. (Fault Tolerance)

بدین منظور مراحل زیر را طی نمایید:

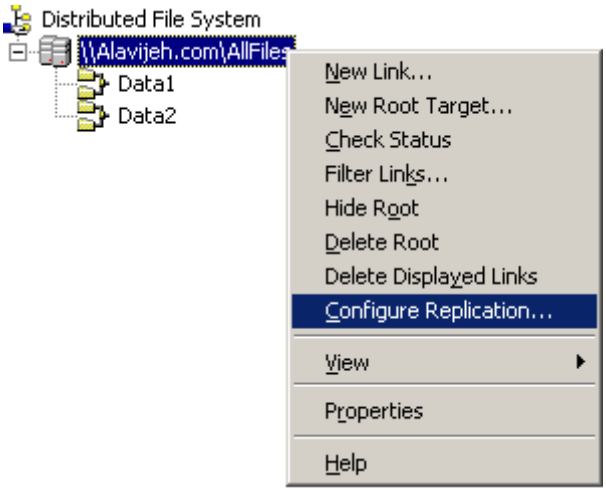
برای ایجاد Fault Tolerance، باید اطلاعات این سرور به پوشه ای عین Root Folder بر روی سروری دیگر منتقل شود. این سرور دوم، بایستی دقیقا مانند همین سرور، قابلیت DFS را داشته باشد؛ یعنی یک ویندوز سرور که همچنین بایستی دارای یک پوشه Share شده، همنام با پوشه Share شده سرور DFS اصلی که به عنوان Root DFS استفاده می شود، باشد. برای شروع، بر روی نام سرور راست کلیک کرده و گزینه New Root Target را انتخاب نمایید.



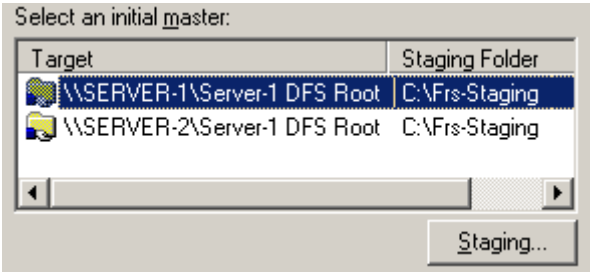
در صفحه باز شده، یکی دیگر از سرور های موجود در Domain را انتخاب نمایید. همانطور که در بالا نیز ذکر شد، ایـن سـرور بایستی دارای سرویس Distributed File System بوده و نیز دارای یک پوشه Share شده، همنام با پوشه Share شـده سـرور DFS اصلی که به عنوان Root DFS استفاده شد، باشد. لذا در صفحه باز شده، روی Browse کلیک کرده و سپس سرور مورد نظر را انتخاب نمایید.



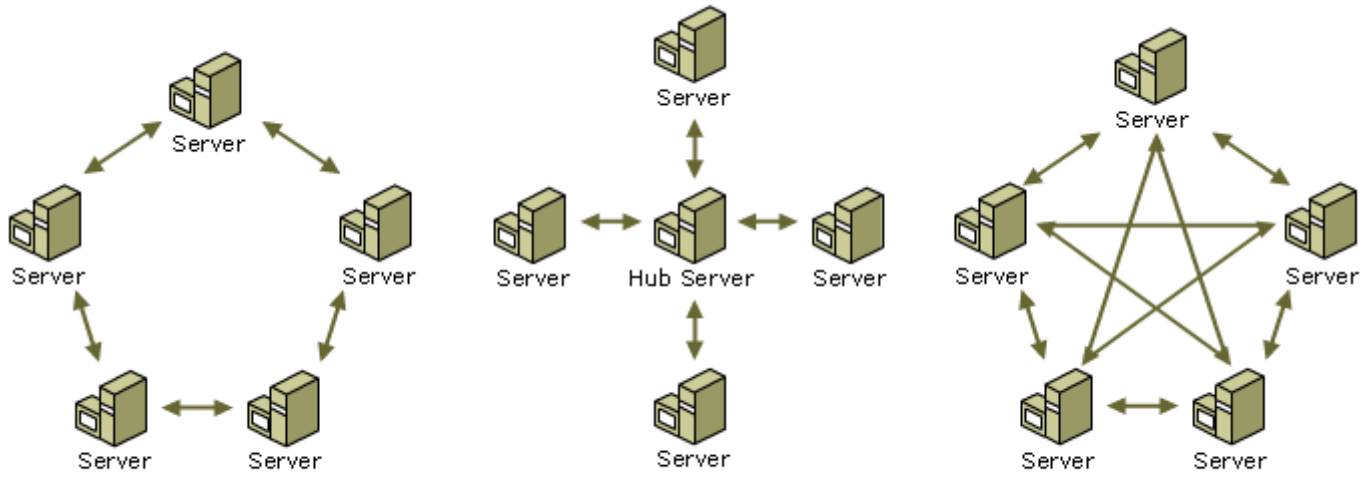
الان ما دو تا سرور داریم که به عنوان DFS Server عمل می کنند. تنها کاری که باید انجام شود، این است که بین این سرور ها Replication راه بیندازیم. برای اینکار دوباره روی نام سرور راست کلیک کرده و سپس گزینـه Configure Replication را انتخاب نمایید.



برای اینکه Replication بتواند صورت بگیرد، سیستم پوشه ای به نام Staging Folder به وجود می آورد تا فایل ها را به صورت موقت در آن نگه دارد. این پوشه را در این صفحه مشخص کنید:



در مرحله ی بعد هم باید اقدام به انتخاب توپولوژی Replication اطلاعات در بین سرور ها کنید که پیشنهاد می کنم از نوع Ring باشد. برای اغلب شبکه ها این توپولوژی بهتر از بقیه جواب می دهد. تصویر زیر تفاوت توپولوژی های مختلف Replication را بهتر نشان می دهد.



فصل ۳۰

Internet Information Service یا IIS

۳۰-۱- معرفی IIS

مسلما تا کنون در ویندوز برنامه های اجرایی با پسوند exe را اجرا کرده اید. اجرای این نوع برنامه ها به سادگی و با رو بار کلیک کردن روی آن ها انجام می گیرد. اما آیا تاکنون به این فکر افتاده اید که چگونه می توان وب سایت های تولید شده با تکنولوژی ASP.Net را بدون کمک Microsoft Visual Studio اجرا کرد؟ ویندوز، سرویسی به نام "سرویس اطلاعاتی اینترنت" یا به اختصار IIS (Internet Information Service) دارد که سرویس هایی جهت انجام امور ارتباطی برای شما فراهم می کند که از جمله آن ها، امکان راه اندازی وب سایت است.

برخی سرویس های IIS عبارتند از:

۱. **HTTP (Hyper Text Transfer Protocol)**: توسط این سرویس می توانید وب سایت های خود را اجرا کرده و آن ها را مشاهده نمایید.
۲. **FTP (File Transfer Protocol)**: این سرویس، خدمات انتقال فایل را ارائه می کند.
۳. **SMTP (Simple Mail Transfer Protocol)**: این سرویس، خدمات ارسال ایمیل را ارائه می کند.
۴. **NNTP (Network News Transfer Protocol)**: این سرویس خدمت ایجاد گروه های خبری و شرکت کاربران در مباحث گفتگویی را فراهم می کند.

در این فصل فقط به معرفی پروتکل HTTP و تنظیمات آن می پردازیم.

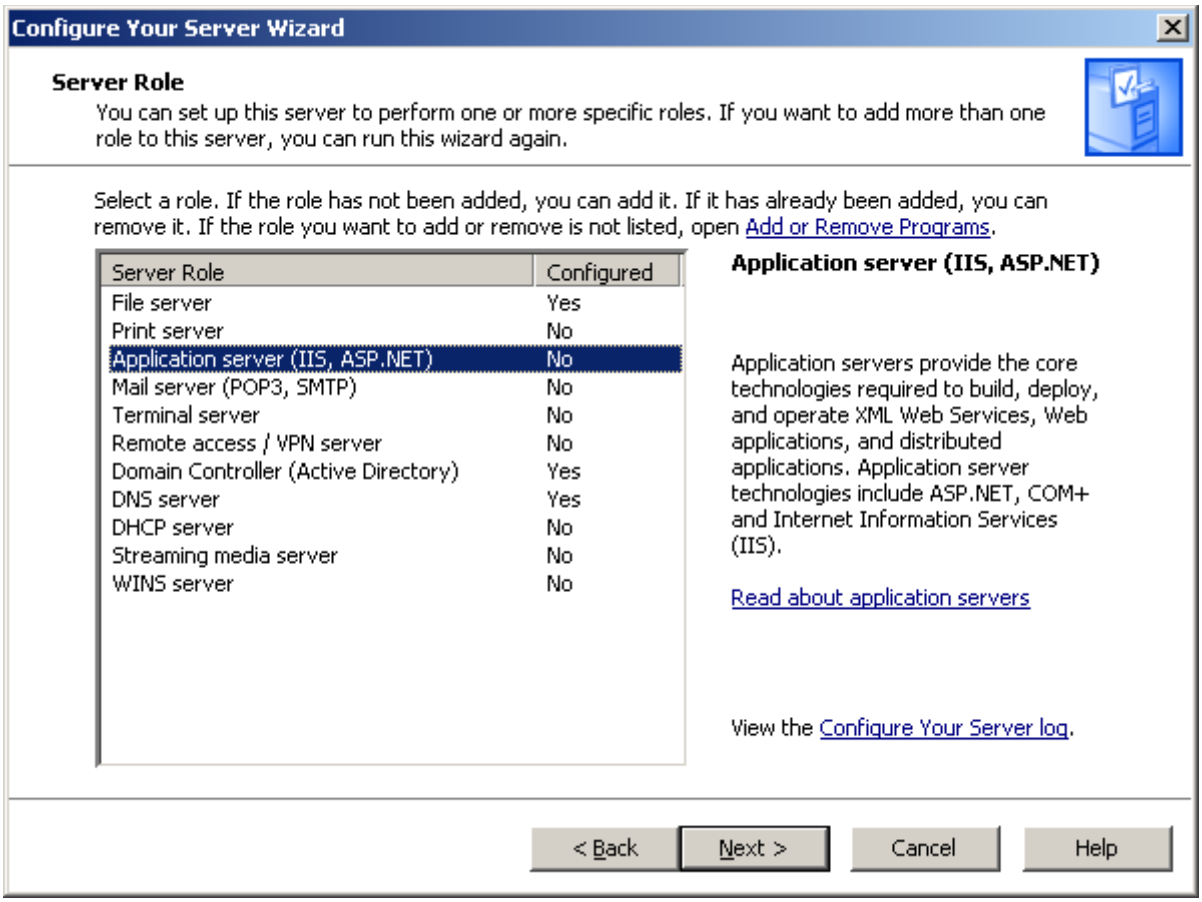
۳۰-۲- نصب IIS

جهت نصب IIS، دو روش وجود دارد که شخصا روش اول را بیشتر ترجیح می دهم. البته روش دوم امکانات بیشتری را در اختیار قرار می دهد.

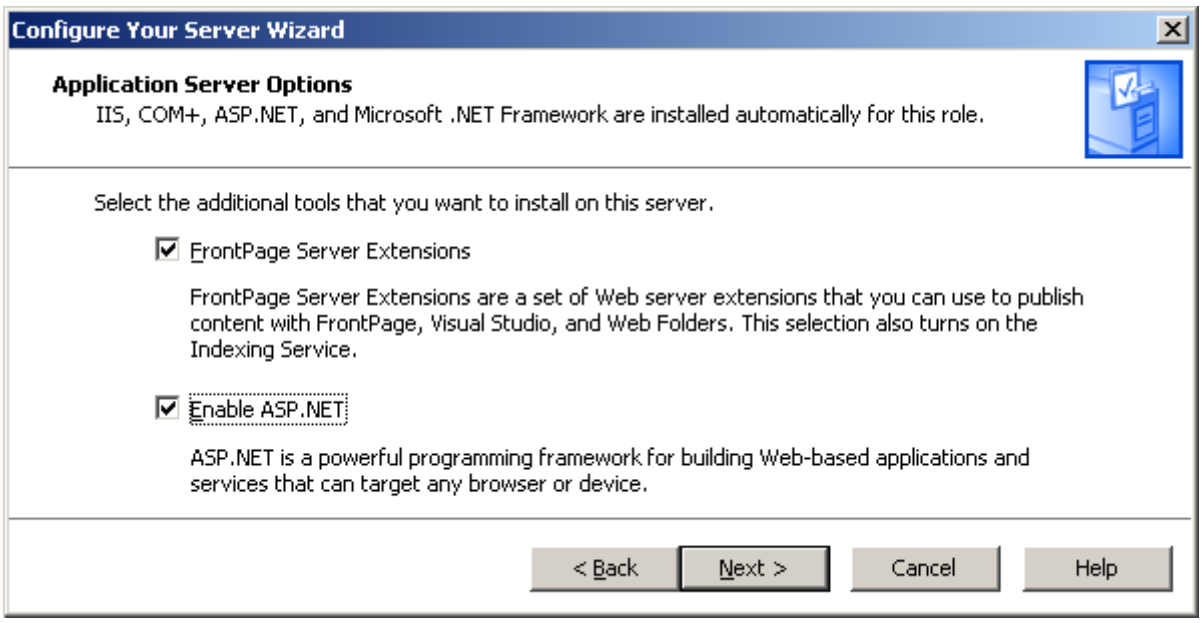
روش اول: بدین منظور ابتدا از مسیر Start ➔ Administrative Tools برنامه Configure Your Server Wizard را اجرا کنید:

در صفحه باز شده دو بار Next را بزنید:

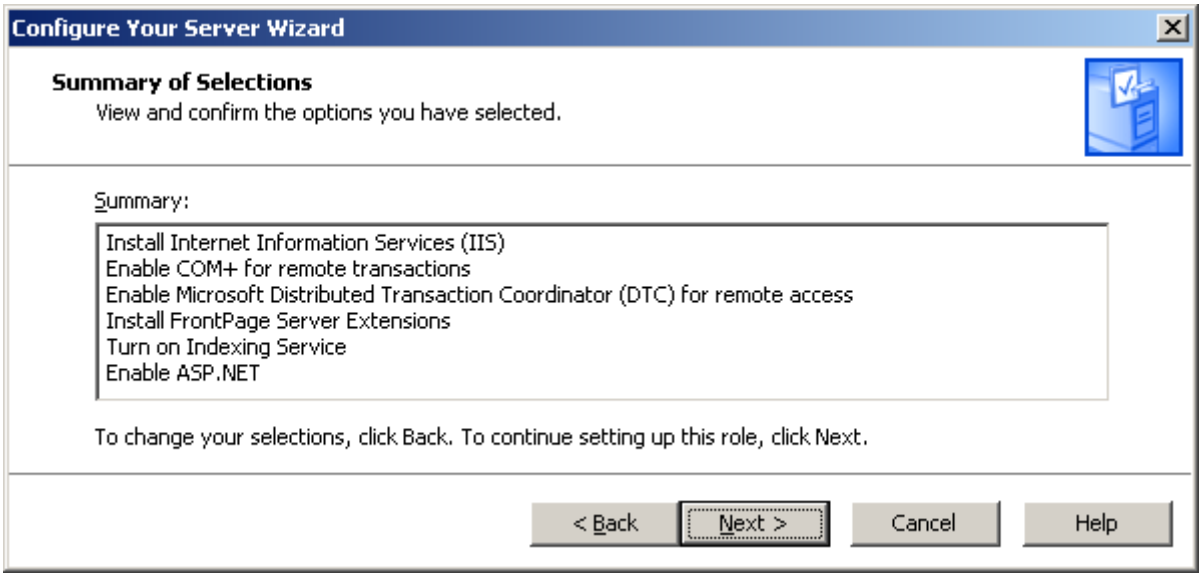
سپس در صفحه باز شده گزینه Application Server را انتخاب نمایید تا این نقش را به نقش های سرور اضافه کنید. سپس روی Next کلیک کنید.



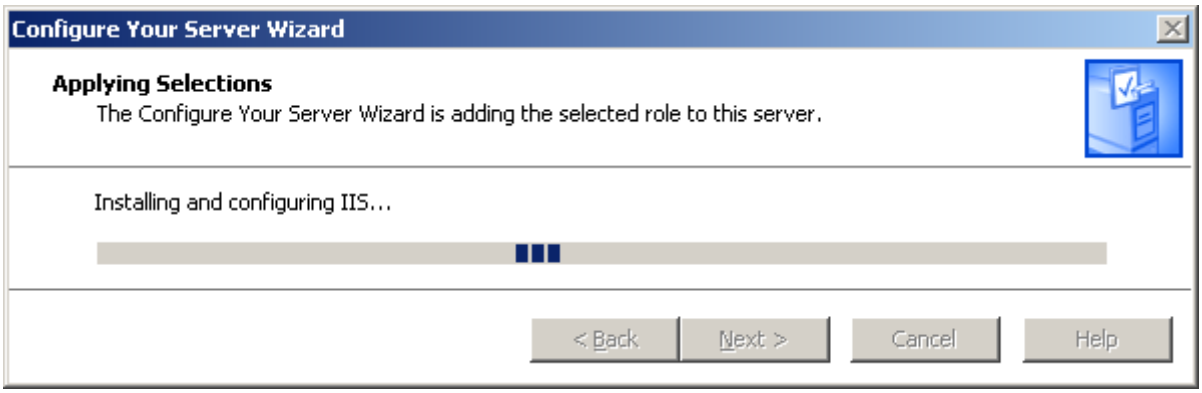
در صفحه بعد، هر دو گزینه FrontPage Server Extensions و Enable ASP.Net را فعال کرده و سپس روی دکمه Next کلیک کنید. دلیل فعال نمودن این دو گزینه این است که سرور بتواند افزونه های FrontPage و فایل های ASP.Net را به عنوان صفحات وب ترجمه نموده و اجرا نماید.



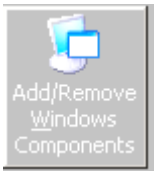
در پایان می توانید خلاصه ای از موارد قابل نصب را مشاهده کنید. جهت نصب روی Next کلیک کنید.



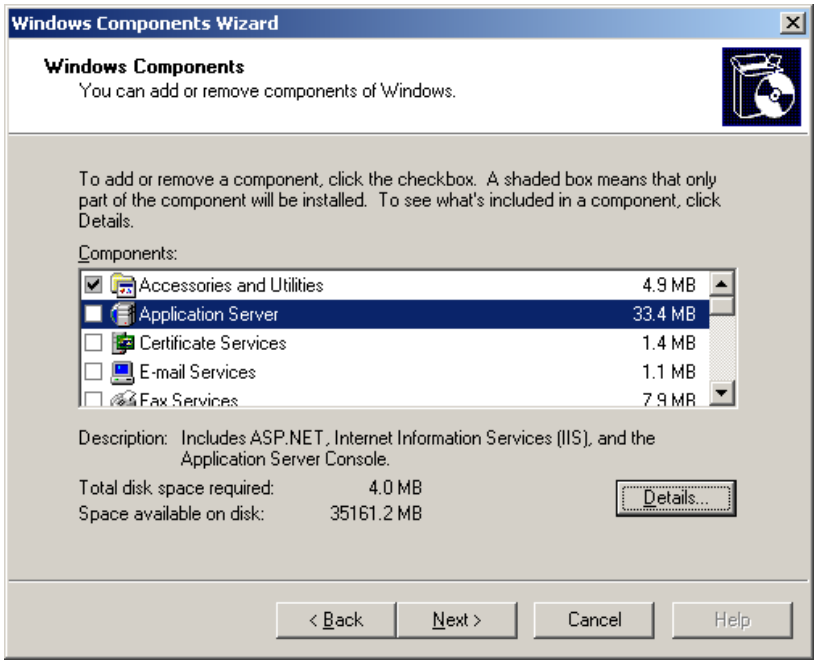
صبر نمایید تا عملیات نصب به پایان برسد. در نهایت روی Finish کلیک کنید.



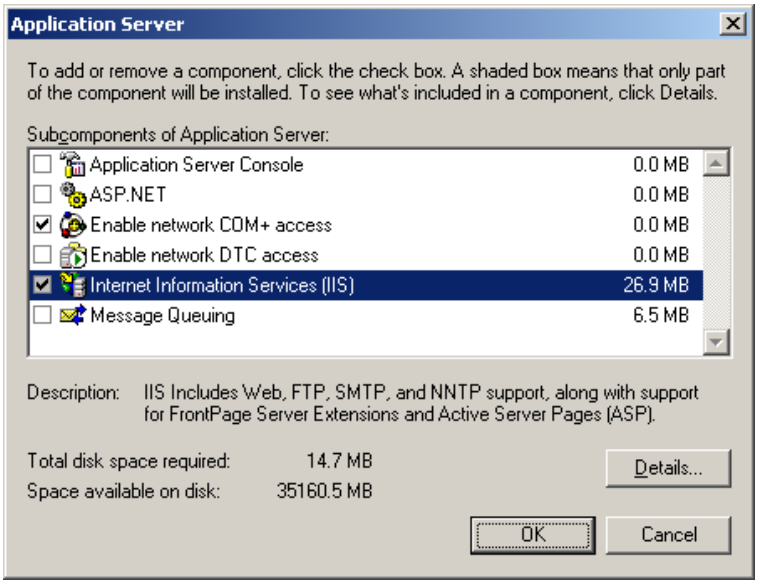
روش دوم: ابتدا وارد Control Panel ➔ Add/Remove Programs شده و سپس روی دکمه Add/Remove Windows Components کلیک کنید تا عناصر ویندوز را مشاهده نمایید.



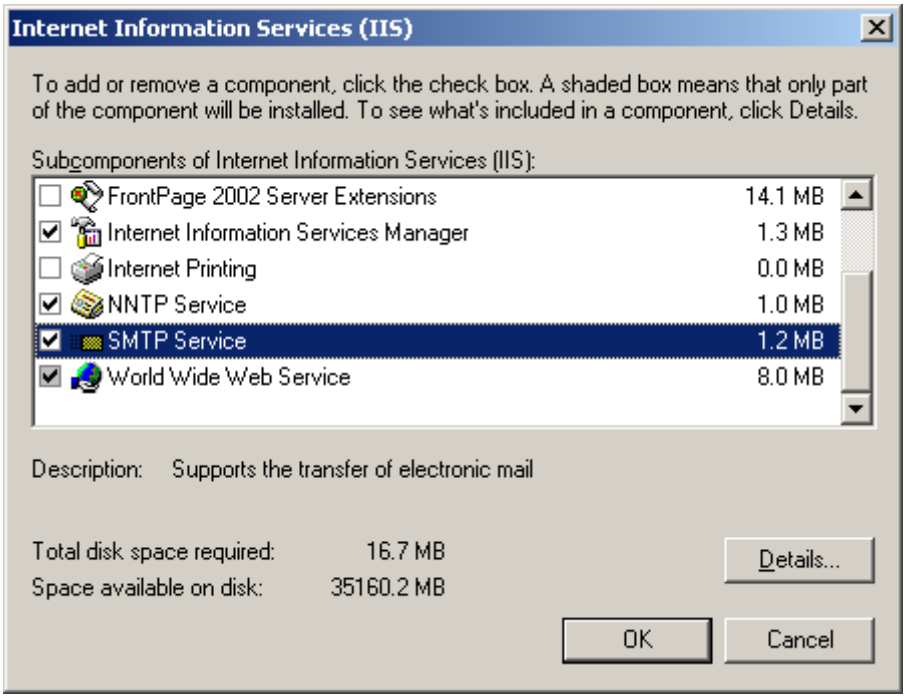
سپس در صفحه باز شده (مانند شکل زیر) گزینه Application Server را انتخاب کرده (توجه: تیک آن را فعال نکنید) و سپس روی دکمه Details کلیک کنید تا امکانات Application Server را مشاهده نمایید.



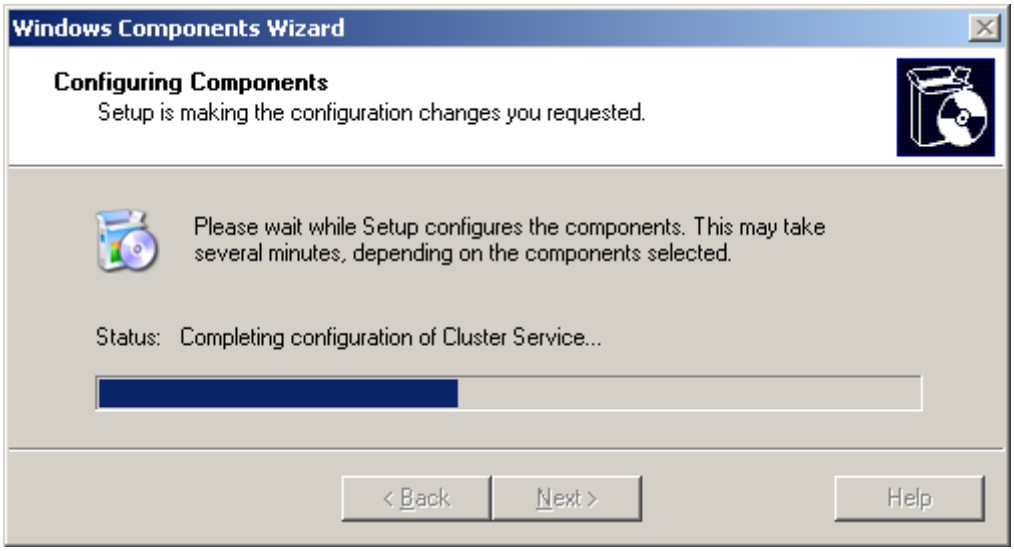
مجددا در صفحه باز شده تیک گزینه Internet Information Services (IIS) را فعال کرده و سپس روی دکمه Details کلیک کنید تا امکانات IIS را مشاهده کرده و آن ها را برای نصب انتخاب کنید.



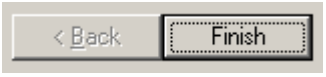
در صفحه باز شده، سرویس های مورد نظر را برای نصب انتخاب کنید. سعی کنید که هر ۴ سرویس معرفی شده در فوق (HTTP، FTP، SMTP و NNTP) را انتخاب و نصب نمایید. سپس روی OK کلیک کنید تا عملیات نصب شروع شود.



صبر نمایید تا عملیات نصب اتمام یابد. احتمالا در هنگام نصب به CD ویندوز نیاز خواهید داشت.

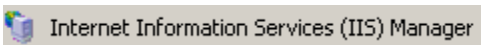


پس از نصب، روی دکمه Finish کلیک کنید تا عملیات نصب خاتمه یابد.

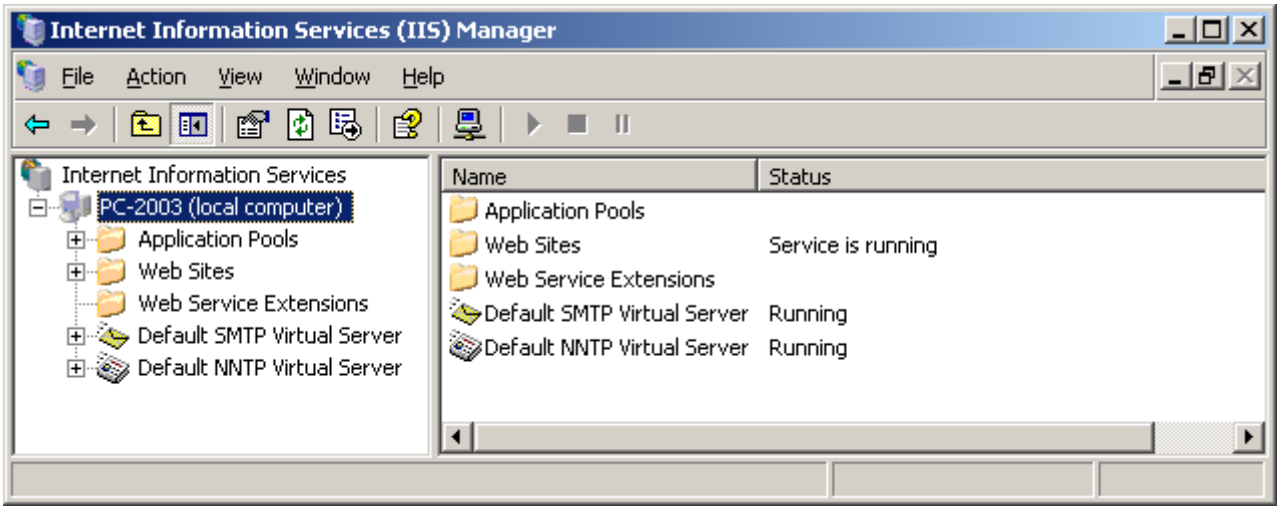


۳۰-۳- اجرا و پیکربندی IIS

جهت اجرای IIS، از مسیر Administrative Tools ➔ Start، گزینه Internet Information Service (IIS) Manager را انتخاب نمایید.

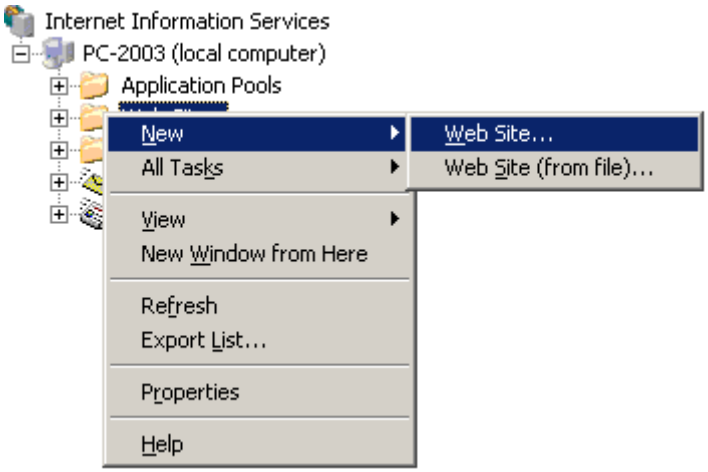


پس از اجرا، صفحه اصلی IIS را مشاهده می بینید که در سمت چپ، ابتدا نام سرور و سپس سرویس های نصب شده را مشاهده خواهید نمود. بخش Web Sites جهت راه اندازی وب سایت می باشد.



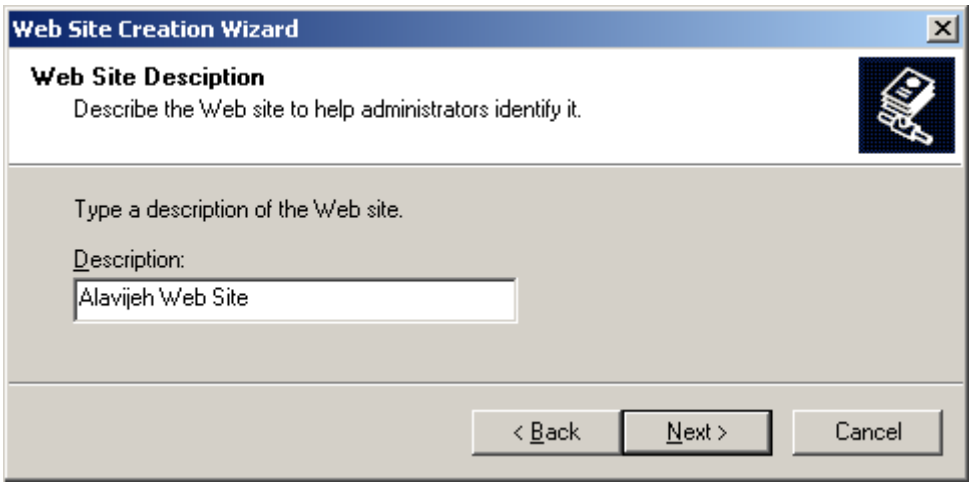
۳۰-۳-۱- تعریف Web Site جدید

جهت ایجاد وب سایت جدید، بر روی بخش Web Sites راست کلیک کرده و سپس گزینه New ➔ Web Site را انتخاب کنید.

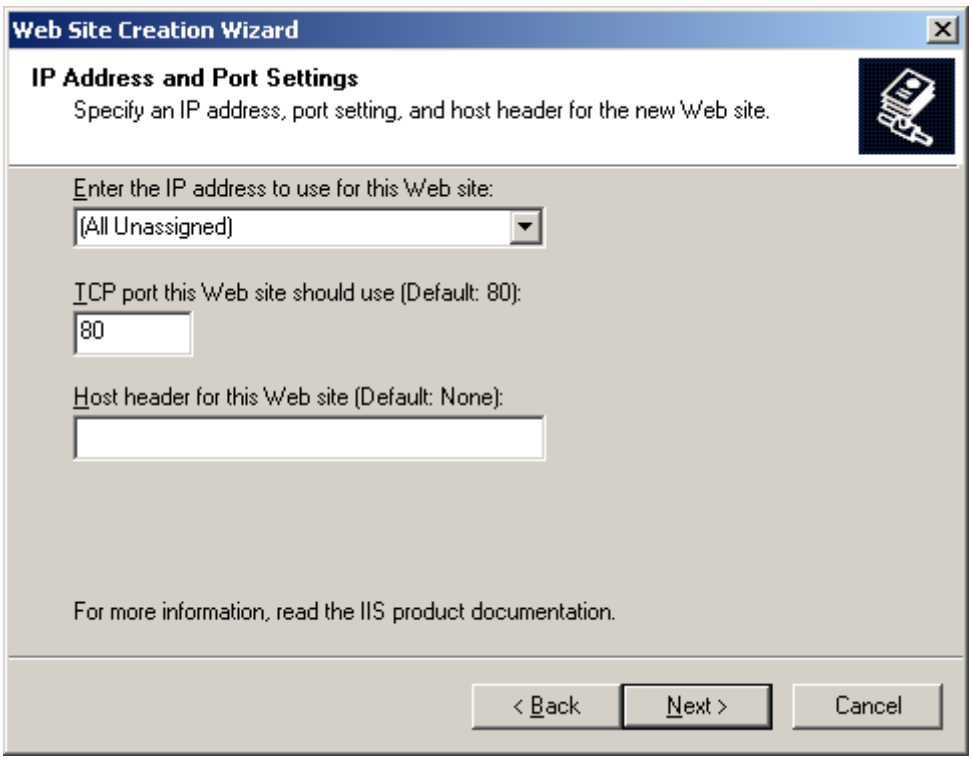


در صفحه خوش آمد گویی، Next را بزنید.

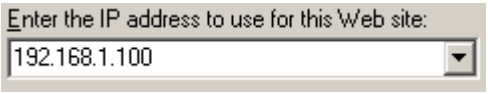
در صفحه بعد، یک **توصیف** (نه نام واقعی) برای وب سایت خود وارد نمایید. این توصیف برای راحتی شما در شناسایی وب سایت های موجود است.



در صفحه بعد، دو تنظیم مهم را باید انجام دهید. یکی آدرس IP است که برای این وب سایت استفاده می شود و به صورت پیش فرض این مقدار برابر All Unassigned است. یعنی با هر آدرس IP که روی سرور تنظیم شده باشد، می توان به وب سایت دسترسی داشت. و تنظیم دیگر، تنظیم پورت مورد استفاده وب سایت است. توجه نمایید که مقدار پورت ها به ازاء وب سایت های ایجاد شده، نباید با هم برابر باشد (توضیح در جلوتر).

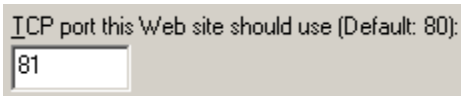


برای تنظیم اول، ما به جای گزینه All Unassigned، از آدرس IP تخصیص داده شده به سرور استفاده می کنیم.

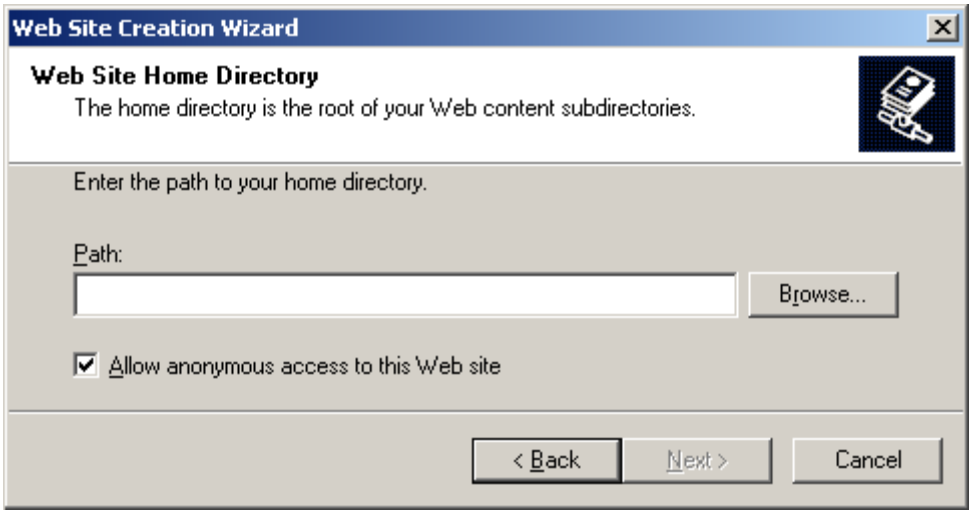


کاربرد تنظیم IP این می باشد که می توان روی سیستم چندین کارت شبکه نصب نمود تا هر سایت از طریق یکی از این کارت شبکه ها به ارائه سرویس بپردازد. همچنین این امکان وجود دارد که چندین سایت از یک کارت شبکه استفاده نمایند.

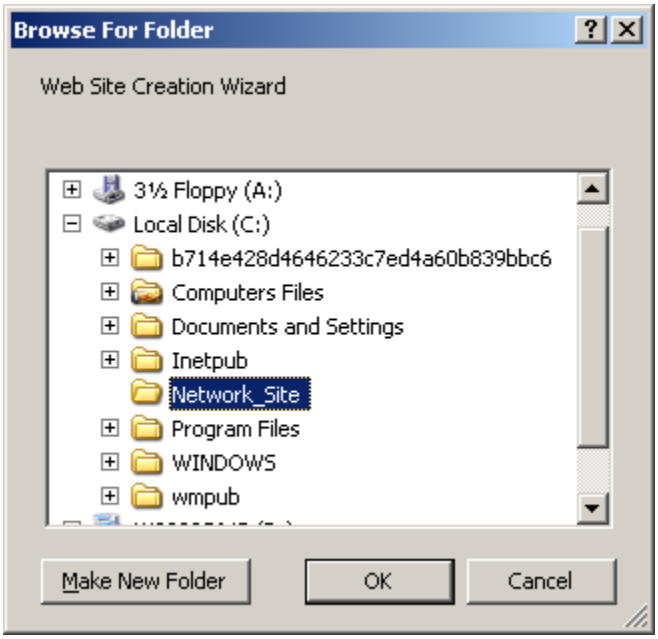
در تنظیم پورت نیز باید توجه داشته باشیم که اگر چند وب سایت تعریف می کنیم، آدرس پورت آن ها نباید با هم برابر باشد. مقدار پورت به صورت پیش فرض ۸۰ است. لذا ما مقدار پورت را ۸۱ یا چیز دیگری تعیین می کنیم. سپس روی دکمه Next کلیک کنید.



در صفحه بعد، مسیری فیزیکی در هارد را تعیین نمایید که فایل های سایت در آن قرار می گیرد. بدین منظور روی دکمه Browse کلیک کنید.



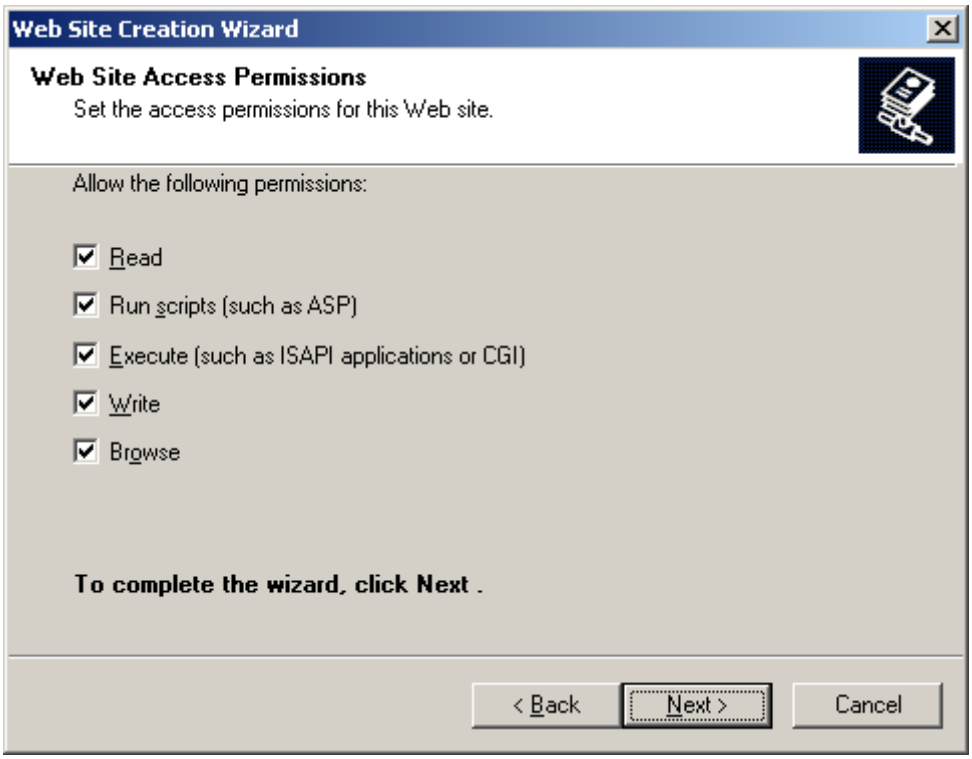
در پنجره باز شده، آدرس فیزیکی خود را انتخاب نمایید. در اینجا، ما مسیر C:\Network_Site را انتخاب نموده ایم.



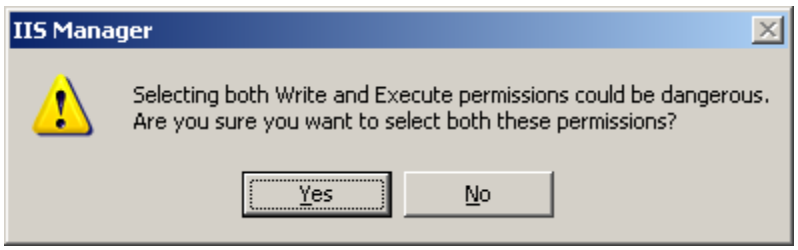
پس از OK کردن، آدرس مسیر فیزیکی را مشاهده خواهید نمود.

نکته: حتما در این صفحه گزینه Allow anonymous access to this Web site را فعال کنید تا کاربران از دیگر کامپیوتر ها بتوانند به وب سایت شما دسترسی یابند. سپس روی Next کلیک کنید.

در این صفحه، سطوح دسترسی سایت خود را تعیین نمایید. مثلاً می توان گفت که این سایت قابلیت ۱- خواندن اطلاعات ۲- اجرای Script (مثل دستورات ASP) 3- اجرای برنامه ها ۴- تغییر اطلاعات و ۵- عمل Browse را داشته باشد. پس از انتخاب Permissionها، روی Next کلیک کنید.



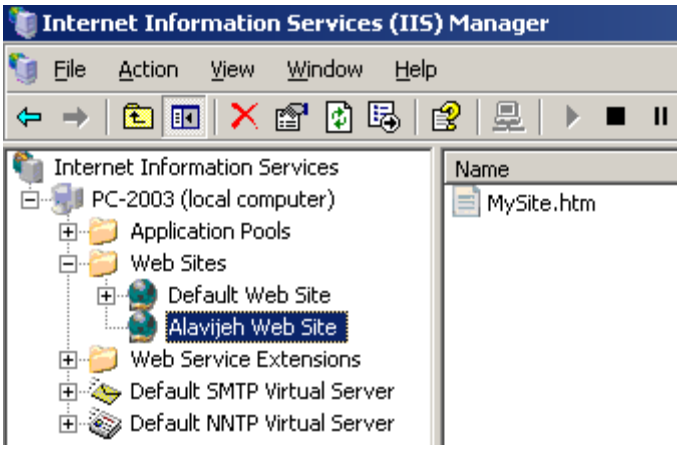
سیستم سوالی در مورد Permissionها و خطر آن ها می پرسد، روی Next کلیک کنید.



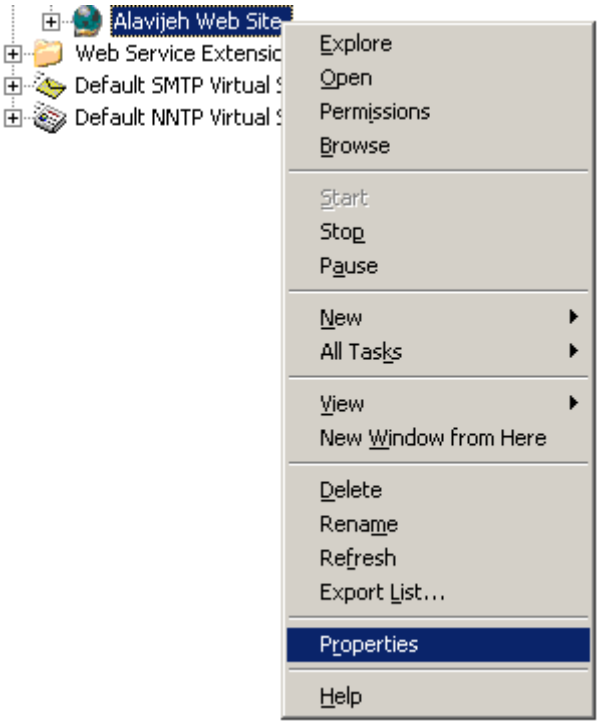
در نهایت روی Finish کلیک کنید تا عملیات ایجاد سایت اتمام یابد.

۳۰-۳-۲- تنظیم وب سایت

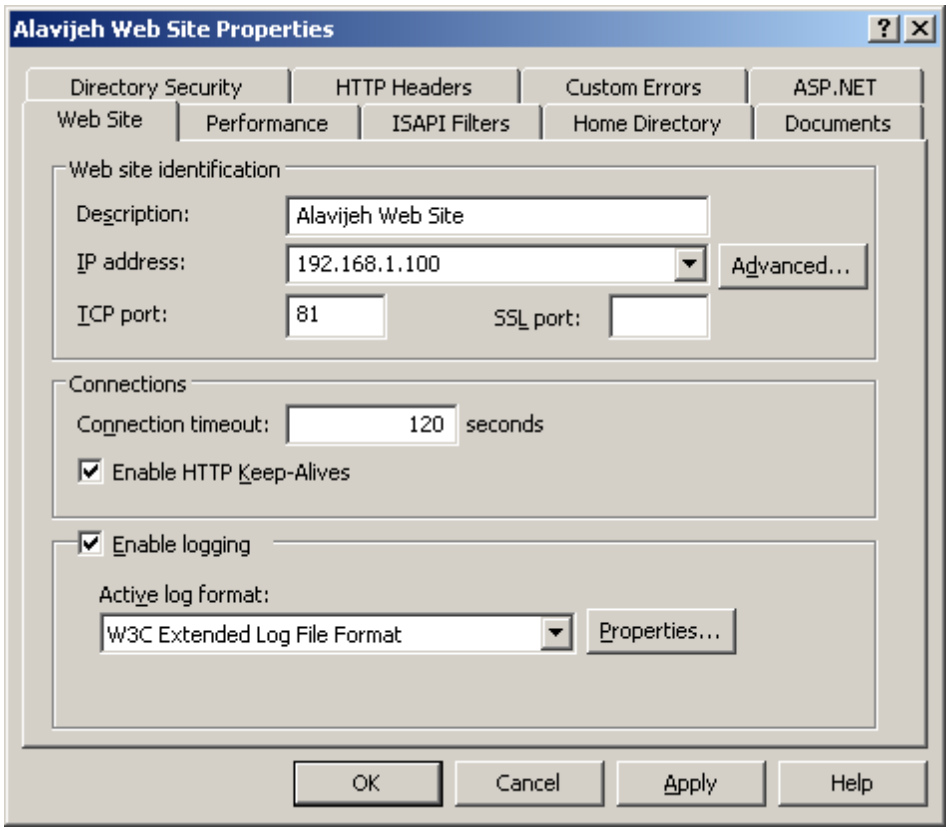
پس از ایجاد وب سایت، فایل های وب سایت خود را در مسیر فیزیکی تعیین شده کپی نمایید. سپس در پنجره IIS، در بخش Web Sites، وب سایت مورد نظر را انتخاب نمایید تا فایل های آن را در سمت راست ببینید.



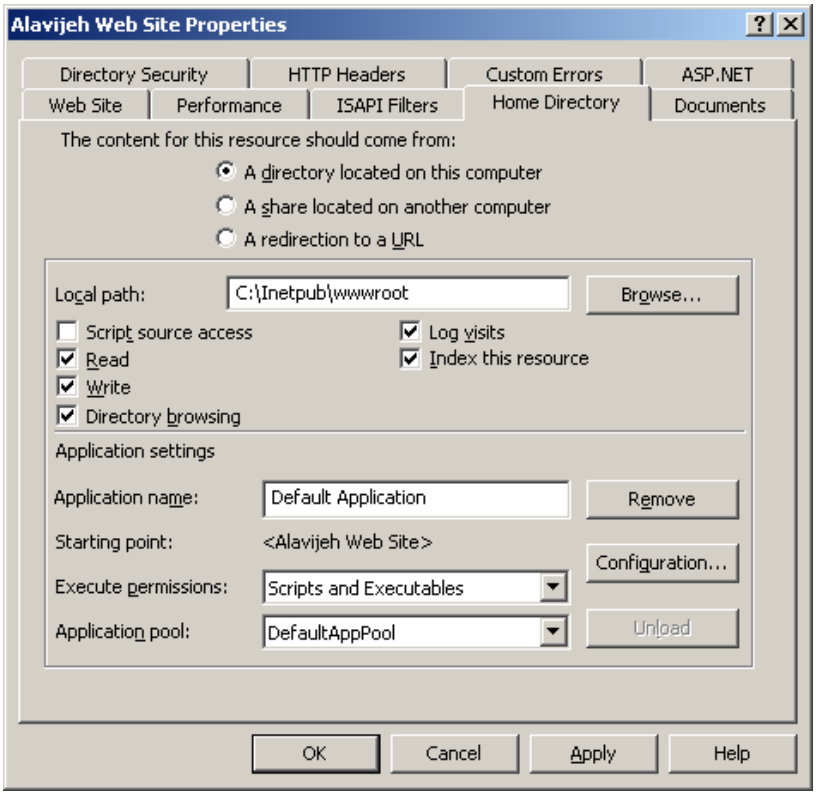
حال قبل از اجرا، نوبت به تنظیمات وب سایت می شود. بدین منظور، روی نام وب سایت راست کلیک کرده و سپس گزینه Properties را انتخاب نمایید.



در پنجره خصوصیات وب سایت، وارد سربرگ Web Site شوید. در این قسمت می توانید تنظیمات اولیه مانند توصیف وب سایت، آدرس IP که برای وب سایت استفاده می شود، پورت مورد استفاده برای وب سایت (توجه نمایید که برای سایت هایی که تعریف می کنید، این آدرس پورت نباید تکراری باشد)، پورت مورد استفاده برای SSL (استفاده از وب سایت در حالت امن) و مقدار Connection Timeout (مدت زمانی که یک اتصال در صورت جواب ندادن باید از بین برود) را تعیین نمایید.

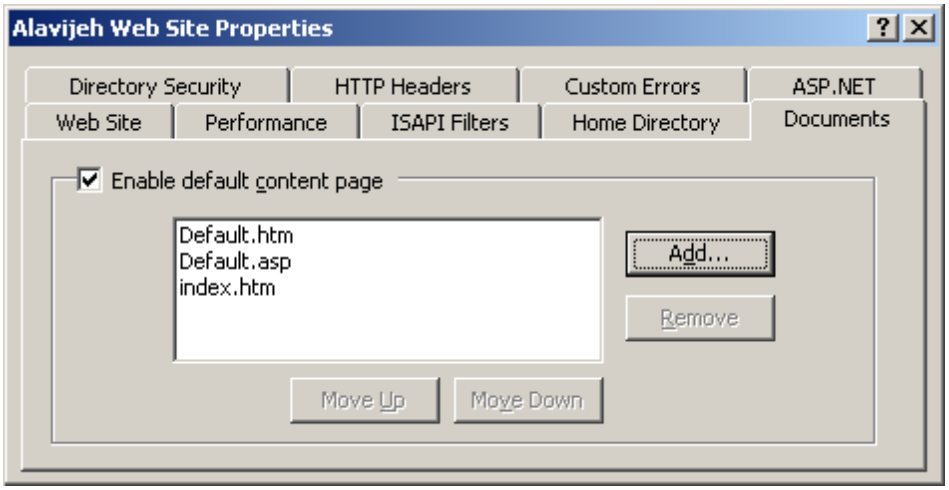


در سربرگ Home Directory می توانید تنظیماتی مانند مسیر فیزیکی فایل های وب سایت و نیز سطوح دسترسی وب سایت را تعیین نمایید.

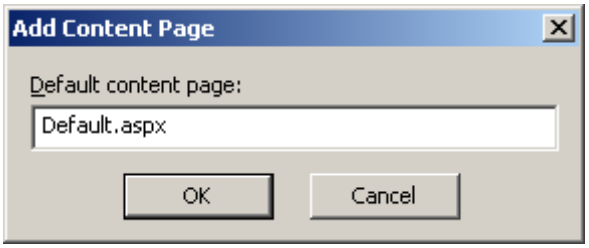


سربرگ Documents، نام فایل های پیش فرضی را مشخص می کند که سیستم هنگام بازکردن وب سایت، در صورتی که نام فایلی را وارد نکرده باشیم، به دنبال این فایل ها می گردد تا آن ها را اجرا کند. در مثال زیر، فرض کنید این تنظیمات را روی وب سایت Google.Com تنظیم کرده ایم. حال پس از وارد کردن آدرس http://www.google.com، سیستم ابتدا دنبال فایل Default.htm می گردد، اگر آن را یافت، آن را اجرا خواهد کرد، و گرنه دنبال فایل Default.asp می گردد تا آن را اجرا کند.

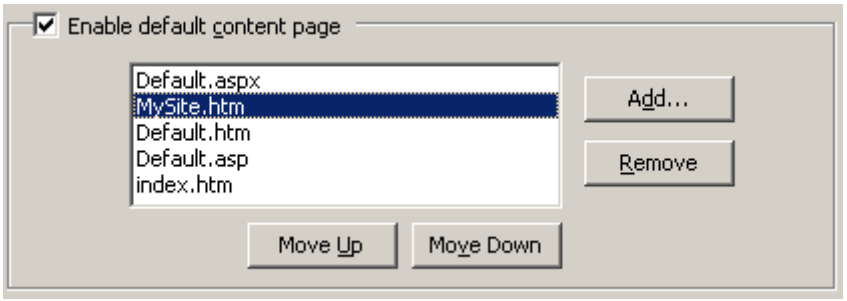
اگر آن را یافت، آن را اجرا خواهد نمود و گرنه دنبال فایل index.htm می گردد. اگر سیستم نتواند این فایل را نیز بیابد، یا وب سایت را در حالت FTP نشان می دهد یا اینکه خطای دسترسی می دهد.



برای افزودن یک فایل پیش فرض جدید، روی دکمه Add کلیک کرده و سپس نام فایل را وارد نمایید.

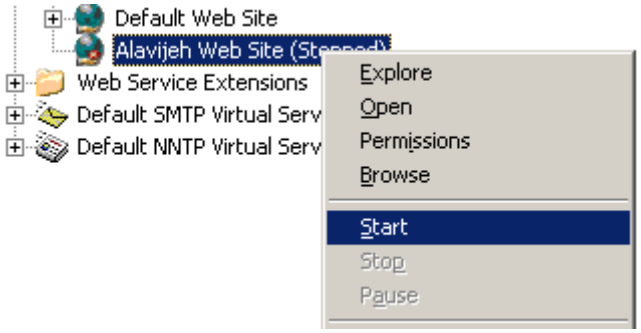


توسط دکمه های Move UP و Move Down نیز می توانید اولویت فایل های پیش فرض برای جستجو و اجرا را تغییر دهید. سپس OK کنید تا پنجره تنظیمات بسته شود.

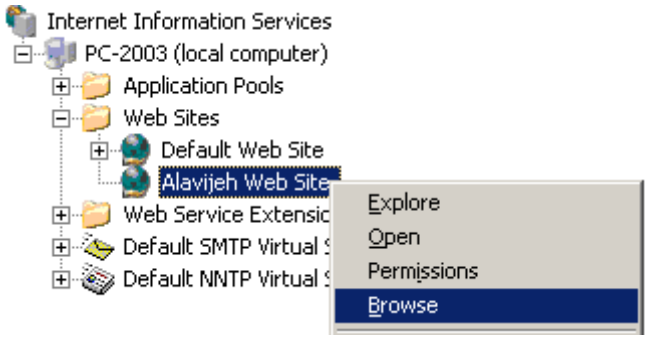


۳۰-۳-۳- اجرای وب سایت

حال برای اجرای وب سایت، ابتدا باید سرویس وب سایت را فعال نمایید. بدین منظور روی نام وب سایت راست کلیک کرده و سپس گزینه Start را انتخاب نمایید.

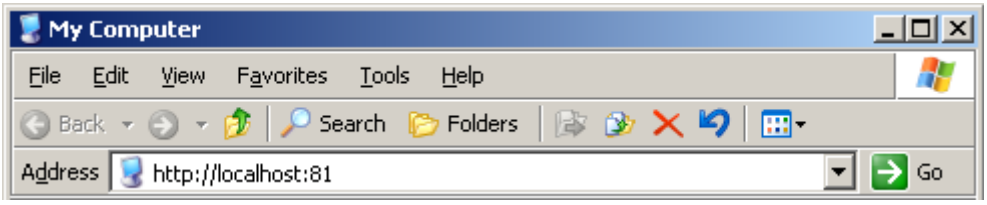


حال برای اجرای وب سایت، روی نام وب سایت راست کلیک کرده و گزینه Browse را انتخاب نمایید.

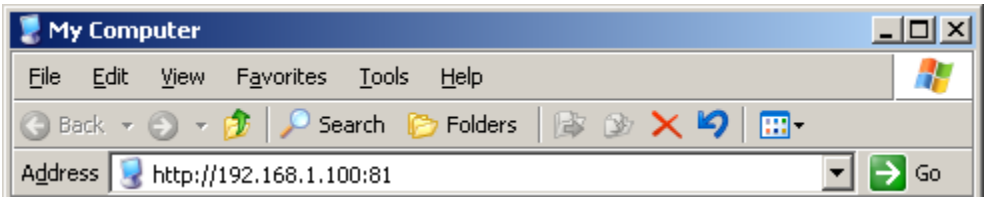


با اینکار، وب سایت اجرا شده را در صفحه IIS مشاهده خواهید نمود.

البته راه دیگری نیز برای اجرای وب سایت وجود دارد. اگر در سیستم خودتان بخواهید وب سایت را اجرا کنید، ابتدا وارد My Computer یا IE شده و سپس آدرس http://LocalHost را به همراه دو نقطه (:) و سپس شماره پورت وب سایت وارد نمایید. مانند شکل زیر:

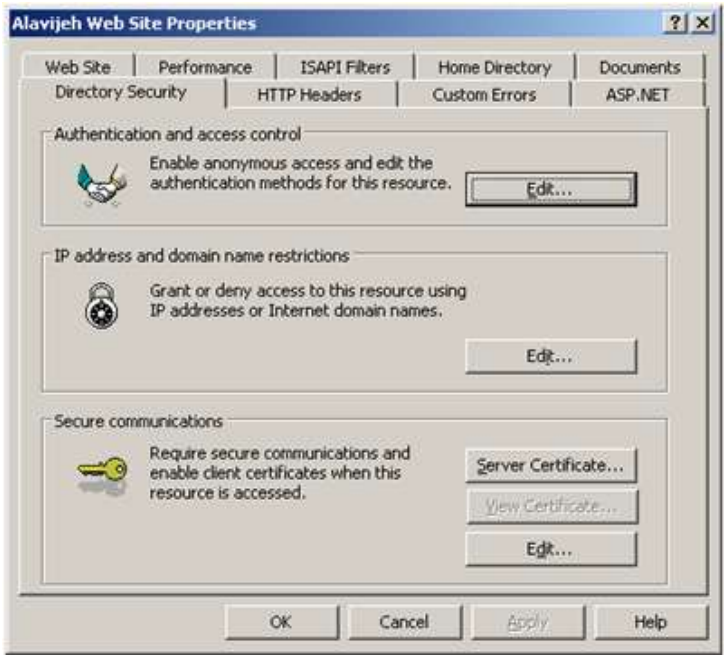


اما اگر بخواهید وب سایت را از سیستمی دیگر اجرا کنید، اینبار به جای LocalHost، آدرس IP مربوط به وب سایت را وارد نمایید.

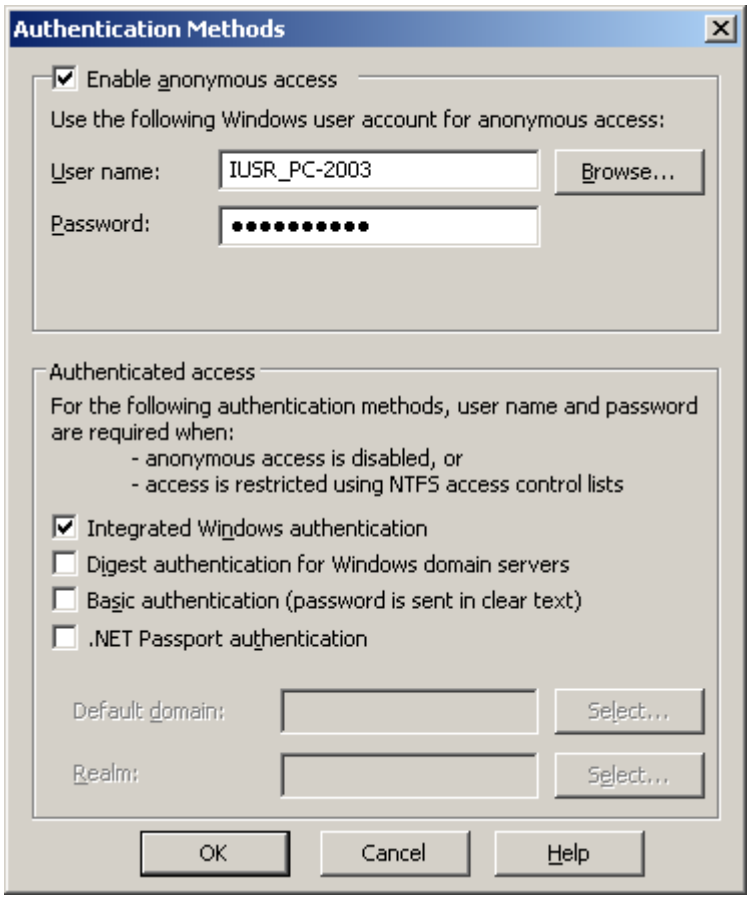


بدین ترتیب وب سایت شما اجرا خواهد شد.

مجددا وارد تنظیمات وب سایت شده و سپس سربرگ Directory Security را انتخاب نمایید. این بخش مربوط بـه تنظیمـات امنیتی می باشد. در این صفحه در قسمت Authentication and access control روی دکمه Edit کلیک کنید تا وارد صفحه تنظیمات دسترسی شوید.



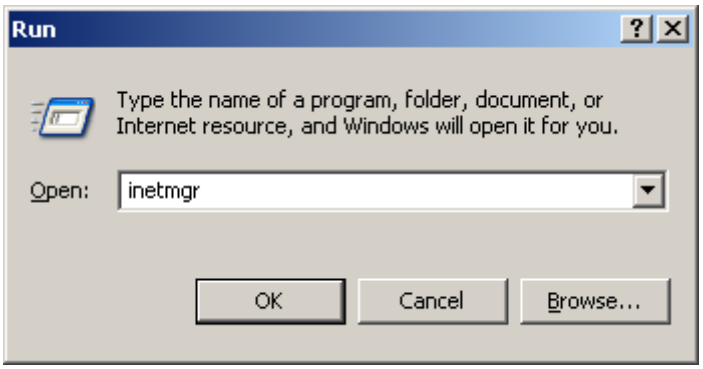
در این صفحه گزینه Enable anonymous access فعال بوده و یک نام کاربری و رمز عبور پیش فـرض نیـز وجـود دارد. ایـن بدان معنا است که کاربران می توانند از راه دور و بدون هیچ Username و Passwordی به وب سایت شما متصل شوند. برای غیر فعال کردن این امکان، تیک گزینه Enable anonymous access را بردارید.



۳۰-۴- اجرای وب سایت های ASP.Net

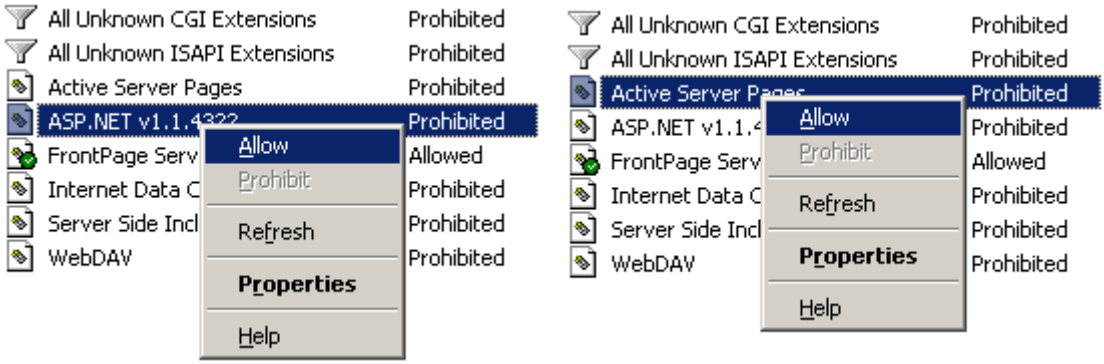
IIS به صورت پیش فرض قابلیت اجرای وب سایت های ASP.Net را نداشته و فقط می تواند وب سایت های HTML را اجرا کند. اگر می خواهید وب سایتی که با تکنولوژی ASP.Net نوشته شده است را روی IIS اجرا کنید، مراحل زیر را دنبال نمایید:

جهت فعال نمودن ASP.Net ابتدا وارد محیط IIS شوید. بدین منظور در Run تایپ کنید: inetmgr



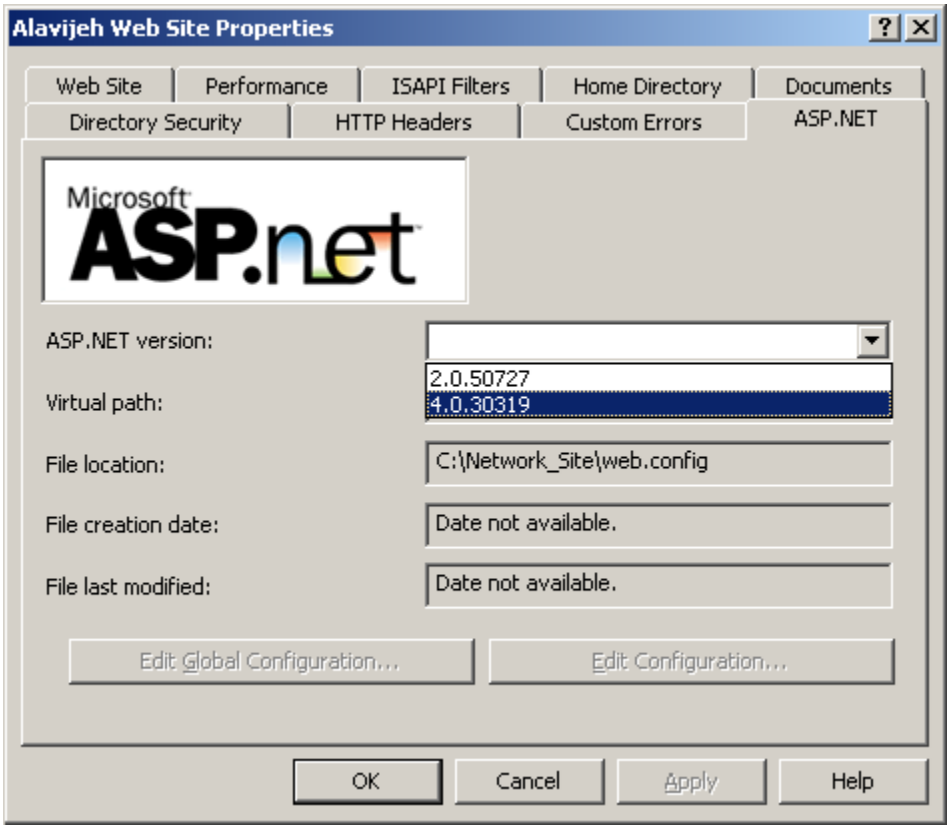
سپس در صفحه باز شده، قسمت Local Computer را بسط داده و سپس Web Service Extensions را انتخاب نمایید.

سپس روی گزینه ASP.Net راست کلیک نموده و سپس گزینه Allow را انتخاب نمایید:

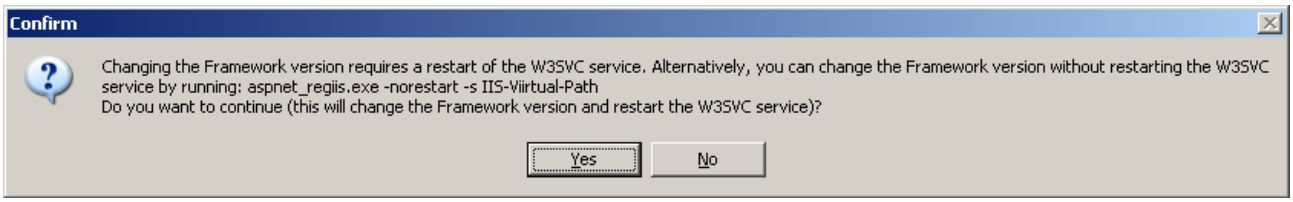


البته اگر نسخه های جدیدتر Framework را نصب کرده باشید، بایستی بتوانید ASP.Net های متناظر را نیز ببینید. سپس آن ها را نیز فعال نمایید.

اگر این کار جواب نداد، یک Framework متناسب با وب سایت خود نصب نمایید. یعنی Framework 1.1 برای Visual Studio 2003، Framework 2.0 برای Visual Studio 2005، Framework 3.5 برای Visual Studio 2008 و Framework 4.0 برای Visual Studio 2010. پس از نصب Framework مناسب، وارد تنظیمات وب سایت شده و سپس سربرگ ASP.Net را انتخاب نمایید. سپس در این قسمت، در بخش ASP.Net version، نسخه ASP.Net خود را انتخاب نمایید.

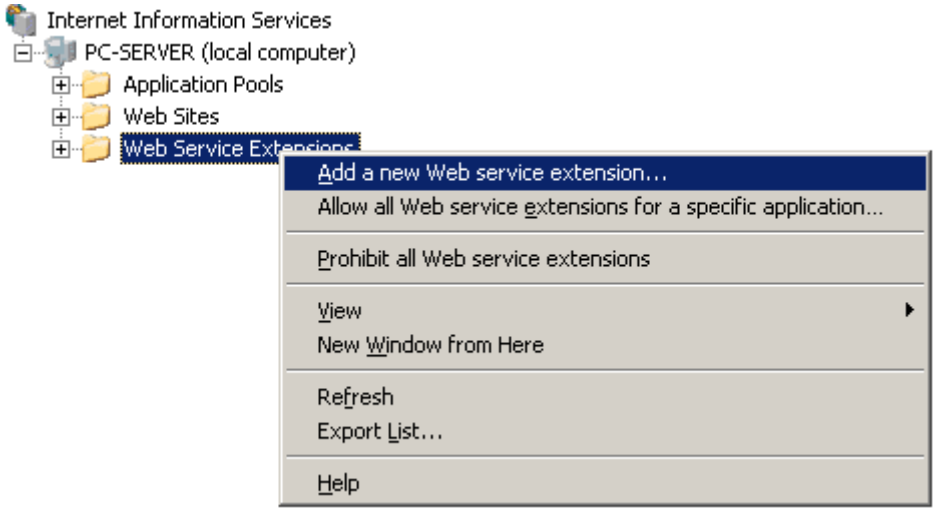


پس از OK کردن، سیستم سوالی از شما می پرسد که دکمه Yes را انتخاب کنید.

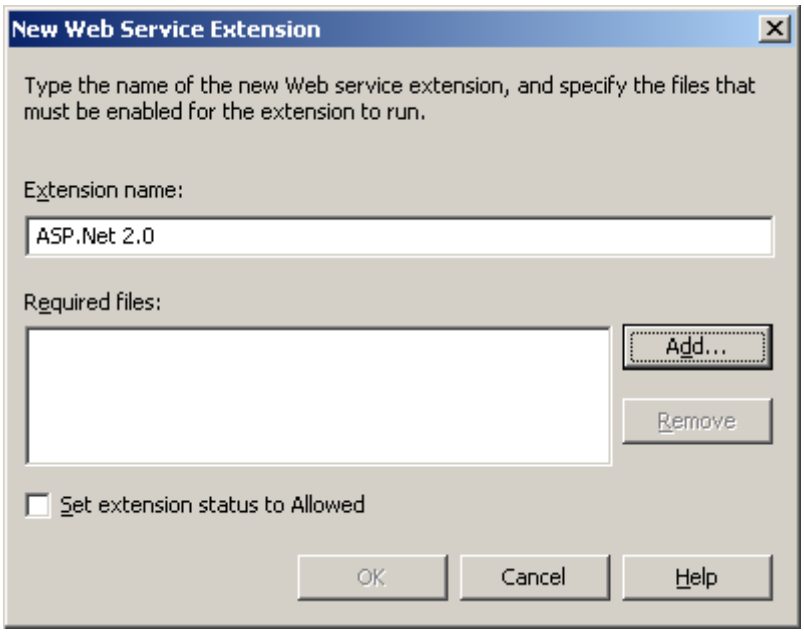


اما اگر بازهم نتوانستید وب سایت ASP.Net خود را اجرا کنید، بایستی یکی از دستورات پیکربندی Visual Studio را اجرا نمایید. ما مثال خود را در Visual Studio 2010 می زنیم. بدین منظور ابتدا وارد Start ➔ Microsoft Visual Studio 2010 ➔ Visual Studio Tools ➔ Visual Studio Command Prompt (2010) شوید. سپس در Visual Studio Command Prompt باز شده، دستور aspnet_regiis –i را اجرا نمایید تا ASP.Net شما روی IIS پیکربندی شود.

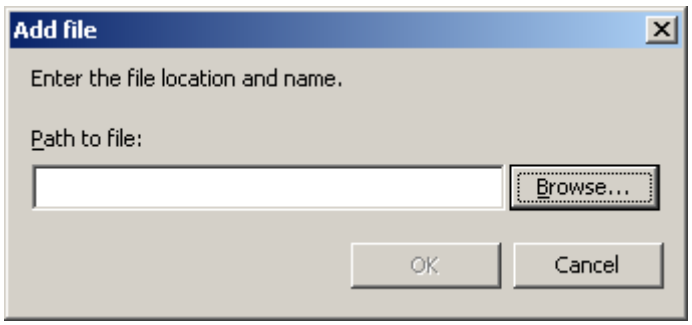
اگر بازهم جواب نداد، ممکن است که مشکل از این باشد که نسخه قدیمی Framework را روی نسخه جدید Framework نصب کرده ایم. برای حل این مشکل، مثلاً برای اجرای ASP.Net 2.0، ابتدا وارد IIS شده و سپس Web Service Extensions را انتخاب کنید. اگر گزینه ASP.Net 2.0 را ندیدید، مشکل نصب Framework قدیمی روی Framework جدید است. لذا برای حل مشکل، روی Web Service Extensions راست کلیک نموده و گزینه Add a new Web service extension را انتخاب نمایید:



سپس نام ASP.Net 2.0 را وارد نموده و روی دکمه Add کلیک کنید:

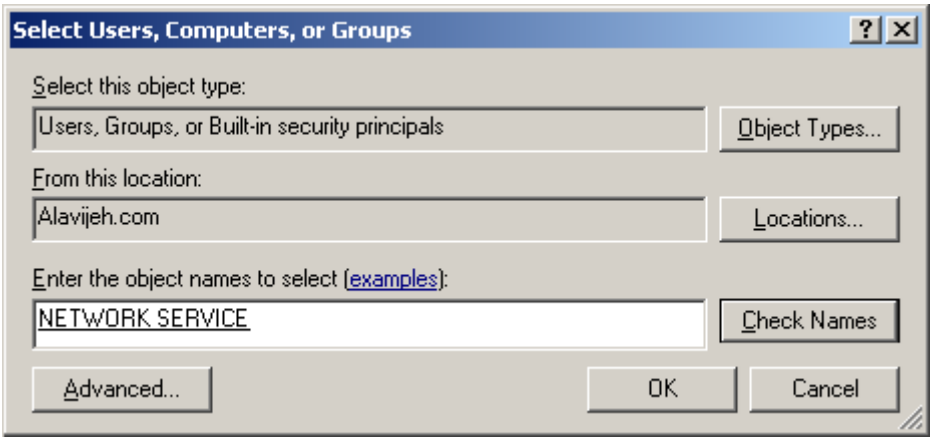


سپس روی دکمه Browse کلیک کنید:

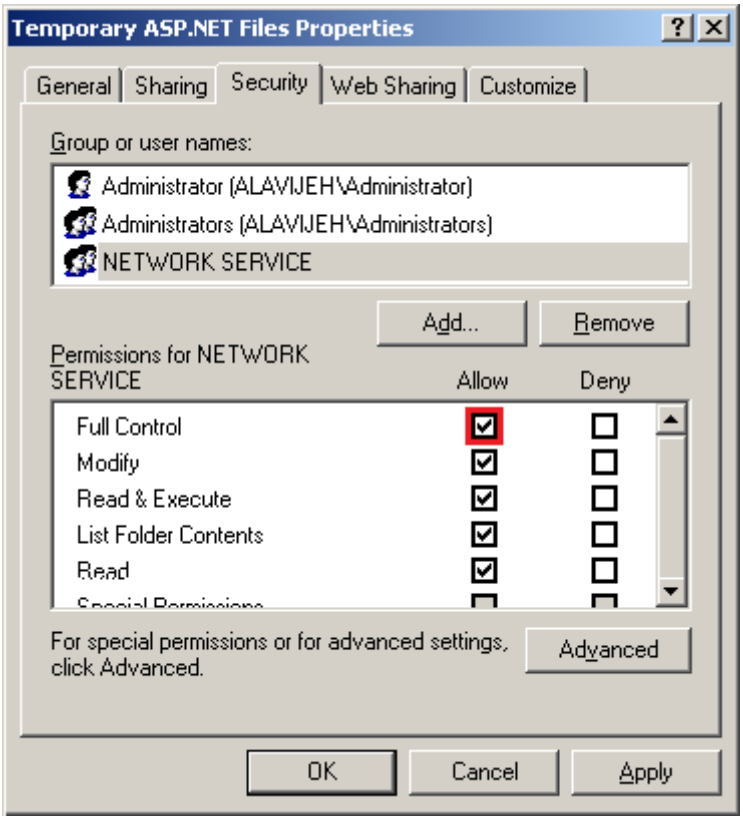


فایل aspnet_isapi.dll را از مسیر C:\Windows\Microsoft.NET\Framework\v2.0.50727 انتخاب نموده و OK کنید. در نهایت مطمئن شوید که وضعیت آن Allow است.

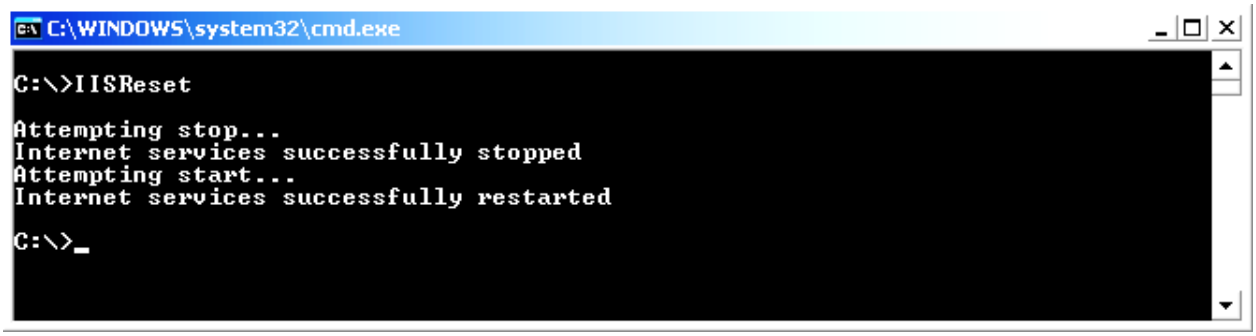
سپس بایستی مطمئن شویم که تمامی کاربران دسترسی کامل به فایل های ASP.Net دارند. لذا پوشه C:\Windows\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET Files را پیدا نموده، روی آن راست کلیک کرده و گزینه Sharing & Security را انتخاب نمایید. سپس وارد سربرگ Security شوید. اگر گزینه Network Service در گزینه ها وجود ندارد، روی Add کلیک نموده، سپس تایپ نمایید Network Service و پس از کلیک روی Check Names، روی دکمه OK کلیک کنید.



سپس در قسمت گزینه های دسترسی، گزینه Full Control را روی Allow تنظیم نموده و سپس روی OK کلیک کنید.



در نهایت برای اعمال تغییرات، IIS را راه اندازی مجدد نمایید. بـدین منظـور در Command Prompt دسـتور IISRESET را تایپ نمایید.



اگر باز هم جواب نداد، یعنی قسمت نیست که ASP.Net روی ویندوز سرور ۲۰۰۳ اجرا شود. لذا از قاعـده "**عامو ولش کن**" شیرازی ها استفاده می کنیم که این قاعده بر هر درد بی درمان دواست!

به پایان آمد این دفتر

حکایت همچنان باقیست

امام صادق (علیه السلام) **فرمودند** :

مَن تَعَلَّمَ العِلمَ وَ عَمِلَ بِهِ وَ عَلَّمَ لِلّهِ دُعِیَ فی مَلَکوتِ السَّماواتِ عَظیما فَقیلَ: تَعَلَّمَ لِلّهِ وَ عَمِلَ لِلّهِ وَ عَلَّمَ لِلّهِ

هر کس برای خدا دانش بیاموزد و به آن عمل کند و به دیگران آموزش دهد، در ملکوت آسمان ها به بزرگی یاد شده و می گویند: **برای خدا آموخت و برای خدا عمل کرد و برای خدا آموزش داد.**

درباره مولف:

مهندس رضا رمضانی در سال ۱۳۸۵ با کسب رتبه ۱۷ کنکور کشوری و رتبه ۱ در استان اصفهان وارد دانشگاه شدند و در سال ۱۳۸۷ موفق شدند رتبه ۴ کشوری در مسابقات علمی کامپیوتر را کسب کنند. همچنین ایشان توانستند در سال ۱۳۸۹ عنوان دانشجوی نخبه را کسب نمایند و سر انجام نیز در همین سال با کسب بالاترین معدل در چهار دوره گذشته از بین دانشجویان رشته مهندسی کامپیوتر فارغ التحصیل شدند. ایشان بلافاصله در سال ۱۳۸۹ وارد مقطع کارشناسی ارشد دانشگاه صنعتی اصفهان شده و در سال ۱۳۹۰ به عنوان رهبر تیم ایران در مسابقات جهانی Max-Sat Evaluation USA 2011 شرکت نمودند (سایت مسابقات جهانی: http://www.maxsat.udl.cat/11/solvers). از زمینه های کاری ایشان می توان Web & Windows Programming، Soft Computing، Parallel Computing، Web Mining، Semantic Web، Linked Data را نام برد. از جمله پروژه های انجامی ایشان نیز می توان به اتوماسیون سازمان صنایع و معادن استان اصفهان، سیستم پزشکی کل استان فارس و مدیریت آزمایشگاه های شرکت هواپیما سازی ایران (هسا) اشاره کرد.