# فهرست

# مقدمه

در این جزوه سعی شده است که مباحث مورد گفتگو در کلاس شبکه‌های ویندوز مبتدی، بطور ساده و قابل درک توضیح داده شود. بر همین اساس، این جزوه را نمی‌توان بعنوان یک مرجع فنی، مورد استفاده قرار داد. بر اساس سیاست‌های بکار گرفته شده در کلاس‌های IT، که دانشجو را تشویق به خودآموزی می‌کند، پیشنهاد می‌شود که این جزوه، تنها بعنوان منبعی جهت یادگیری اولیه استفاده شود و دانشجو خود نسبت به فراگیری کامل این مباحث اقدام نماید.

کلاس شبکه‌های ویندوز مبتدی، بر اساس قابلیت‌های ویندوز ۲۰۰۳، طراحی و اجرا می‌شود. کلیهٔ مراحل توضیح داده شده در این جزوه نیز، با استفاده از این سیستم‌عامل است. ولی با اندکی تغییر، این جزوه را می‌توان با سیستم‌عامل‌های Windows 2000 server و Windows 2000 Advanced server نیز استفاده کرد.

این کلاس، تنها به مباحث نرم‌افزاری طراحی و راه‌اندازی شبکهٔ ویندوز NT می‌پردازد و دانشجو باید خود نسبت به فراگیری نکات سخت‌افزاری اقدام نماید.

این جزوه توسط نرم‌افزار Microsoft word تهیه شده و کلیهٔ عکس‌های بکار رفته توسط نرم‌افزار Microsoft Virtual PC گرفته شده است. سپس توسط نرم‌افزار PDF Factory به فایل PDF تبدیل شده است. سعی می‌شود که جزوهٔ جداگانه‌ای جهت توضیح نرم‌افزار MVPC و PDF Factory تهیه شود.

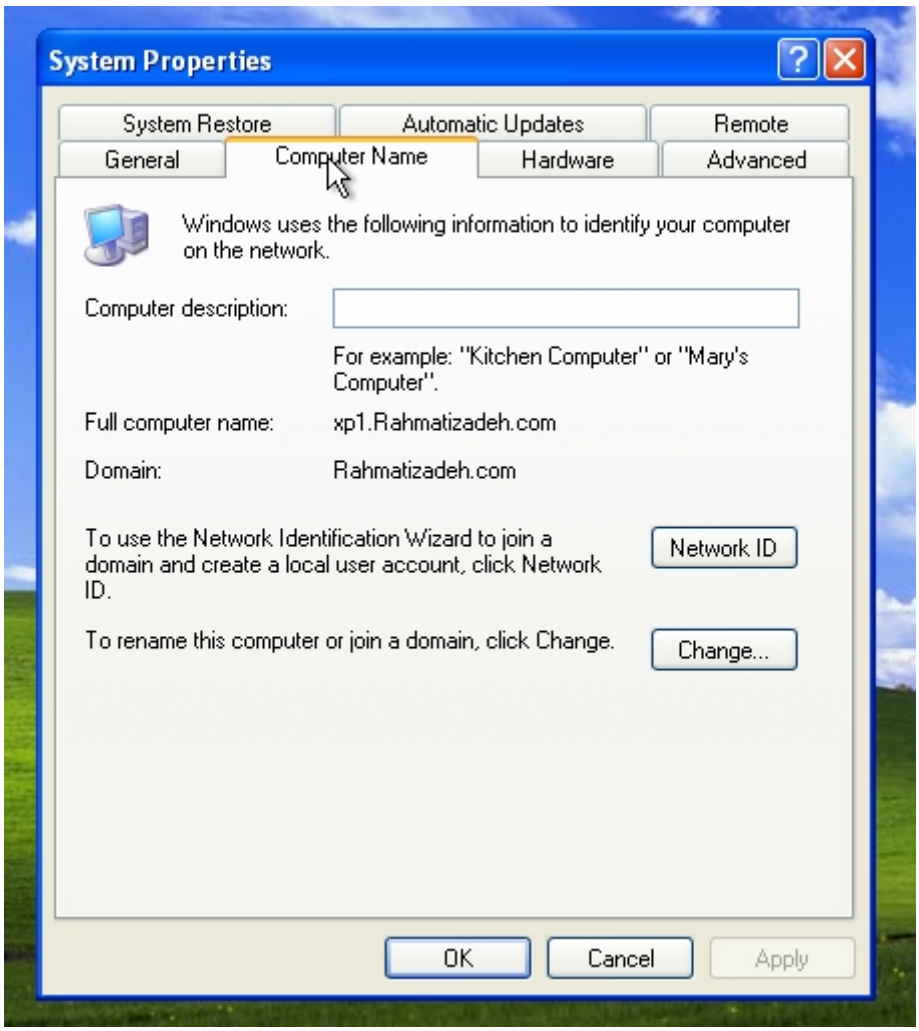
# پیش‌نیازها

در ابتدای این جزوه، لازم است که مباحثی که بصورت پیش‌نیاز برای شروع راه‌اندازی شبکه مـورد نیاز است، بطور اختصار توضیح داده شود:

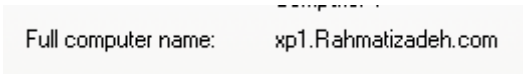
- ***نام کامپیوتر (Computer Name)***

هر کامپیوتر در شبکه، دارای نام منحصر بفرد می‌باشد. از این نـام مـی‌تـوان جهـت ارتبـاط بـا کامپیوتر، در داخل شبکه استفاده کرد. جهت مشاهده یا تغییـر نـام کـامپیوتر، پـس از لاگـین کردن با کاربر Administrator، به روش زیر عمل کنید :


بر روی دکمهٔ Start کلیک کـرده و بـر روی علامـت My Computer، دکمـهٔ سـمت راسـت موس را بزنید. سپس گزینهٔ Properties را انتخاب کنید.

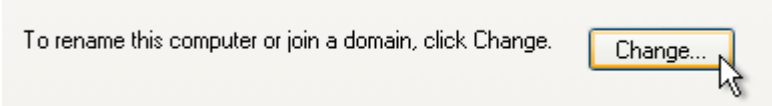


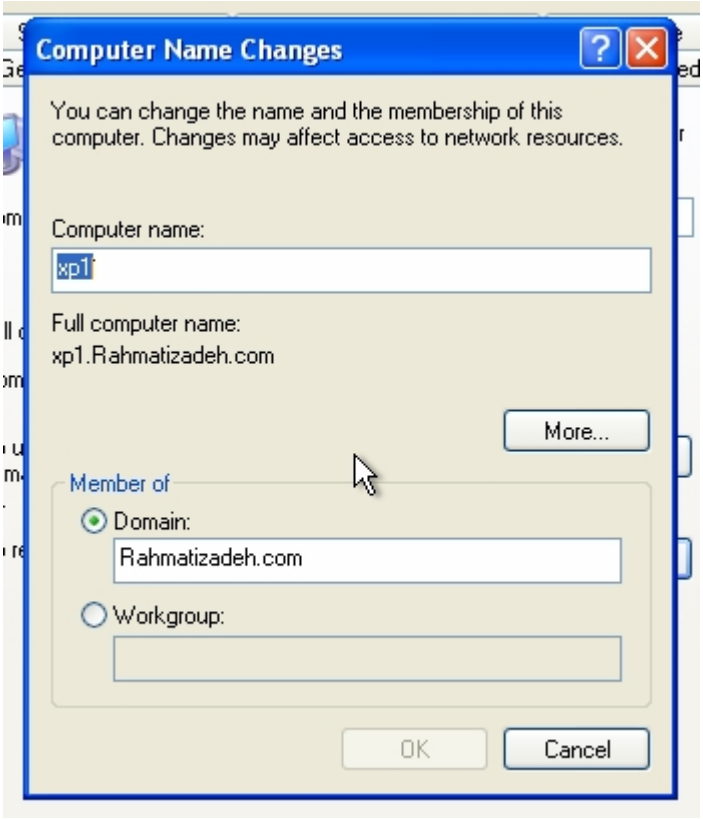

**پس از ظاهر شدن پنجرهٔ** System Properties**، سربرگ** Computer Name **را انتخاب کنید.**




**در قسمت** Full computer name**، نام کامل کامپیوتر را می‌توانید مشاهده کنید. نام کامل کامپیوتر، شامل نام کامپیوتر به همراه** Domain**ای که کامپیوتر در آن عضو می‌باشد است که توسط نقطه از هم جدا شده‌اند. در قسمت‌های بعدی این جزوه در مورد** Domain **توضیح داده خواهد شد. نام کامپیوتری که در شکل آمده است،** "xp1" **بوده که عضو** Domain "Rahmatizadeh.com" **می‌باشد.**

**جهت تغییر نام کامپیوتر بر روی دکمهٔ** Change **کلیک کنید:**






**در قسمت Computer name نام کامپیوتر و در قسمت Domain نام Domainای را که کامپیوتر عضو آن می‌باشد، وارد کنید.**

**در تعویض نام کامپیوتر، نکات زیر را مد نظر داشته باشید :**

a. **جهت تعویض نام کامپیوتر، باید حتما Administrator و یا عضوی از گروه Administrators باشید.**

b. **در صورتیکه کامپیوتر در شبکه باشد، ممکن است سیاست‌های اعمال شده بر روی شبکه، از تغییر نام کامپیوتر جلوگیری کند.**

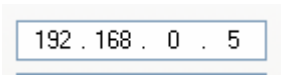
c. **در صورتیکه کامپیوتر عضوی از یک Domain باشد، ممکن است نام و رمز کاربری که اجازهٔ تغییر نام کامپیوتر در Domain را دارد، از شما خواسته شود.**

d. **فقط در شرایط خاص که در توضیحات مربوط به DNS خواهد آمد، طول نام کامپیوتر می‌تواند از ۱۵ حرف بیشتر باشد.**

**پس از تعویض نام کامپیوتر، به شرطی که کامپیوتر هم‌نامی در شبکه وجود نداشته باشد، کامپیوتر باید Restart شده تا نام جدید مورد استفاده قرار گیرد.**

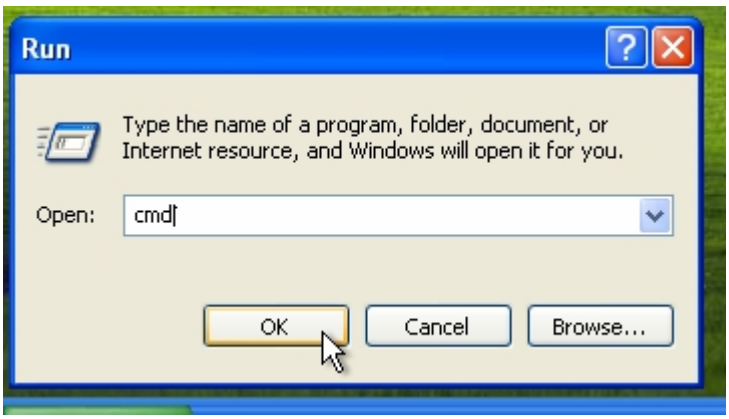
- ***اینترنت پروتوکل یا IP***

**هر کامپیوتر موجود در شبکه، با یک عدد منحصر بفرد شناخته می‌شود. این عدد از چهار قسمت تشکیل شده است که هر قسمت آن توسط نقطه از هم جدا شده و می‌تواند عددی بین صفر و ۲۵۵ باشد. نمونه‌ای از این عدد را در شکل ملاحظه می‌کنید:**

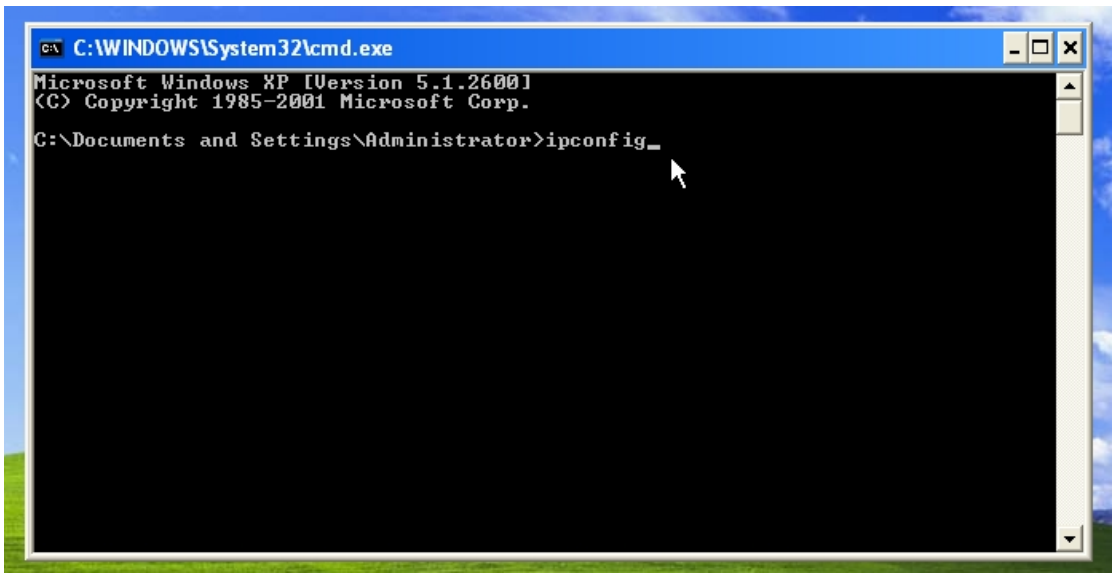


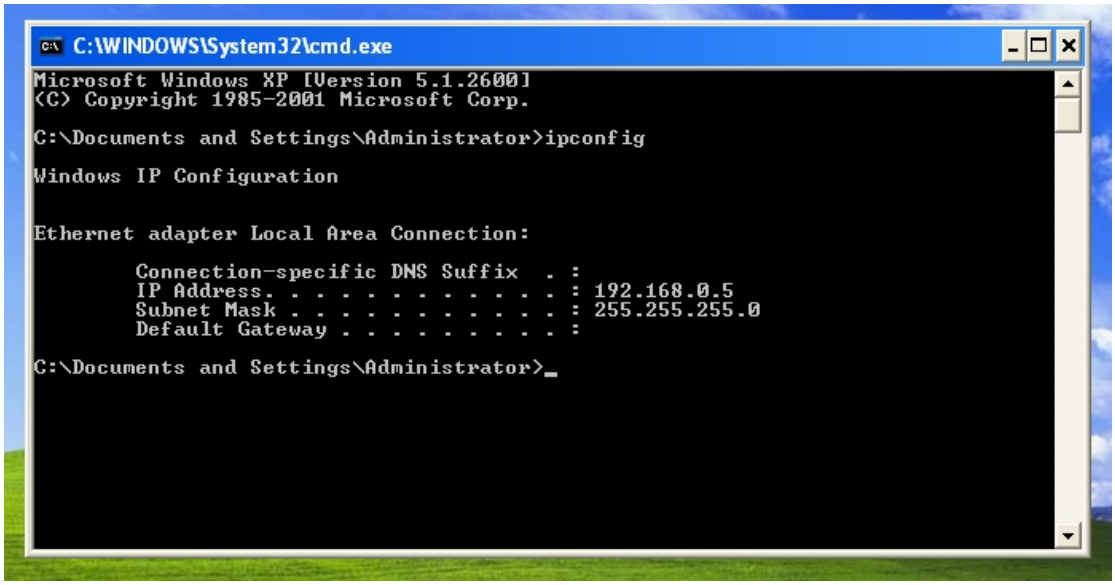

**در حقیقت، این عدد از چهار بایت تشکیل شده که هر بایت نشانگر یک عدد از مجموع چهارعدد فوق است. کامپیوتر از این عدد برای ارتباط برقرار کردن با کامپیوترهای دیگر شبکه استفاده می‌کند. جهت مشاهدهٔ IP کامپیوتر خود به چند روش می‌توانید عمل کنید:**

**در روش اول از منوی Start گزینهٔ Run را انتخا کنید و کلمهٔ cmd را تایپ کنید و کلید OK را فشار دهید.**



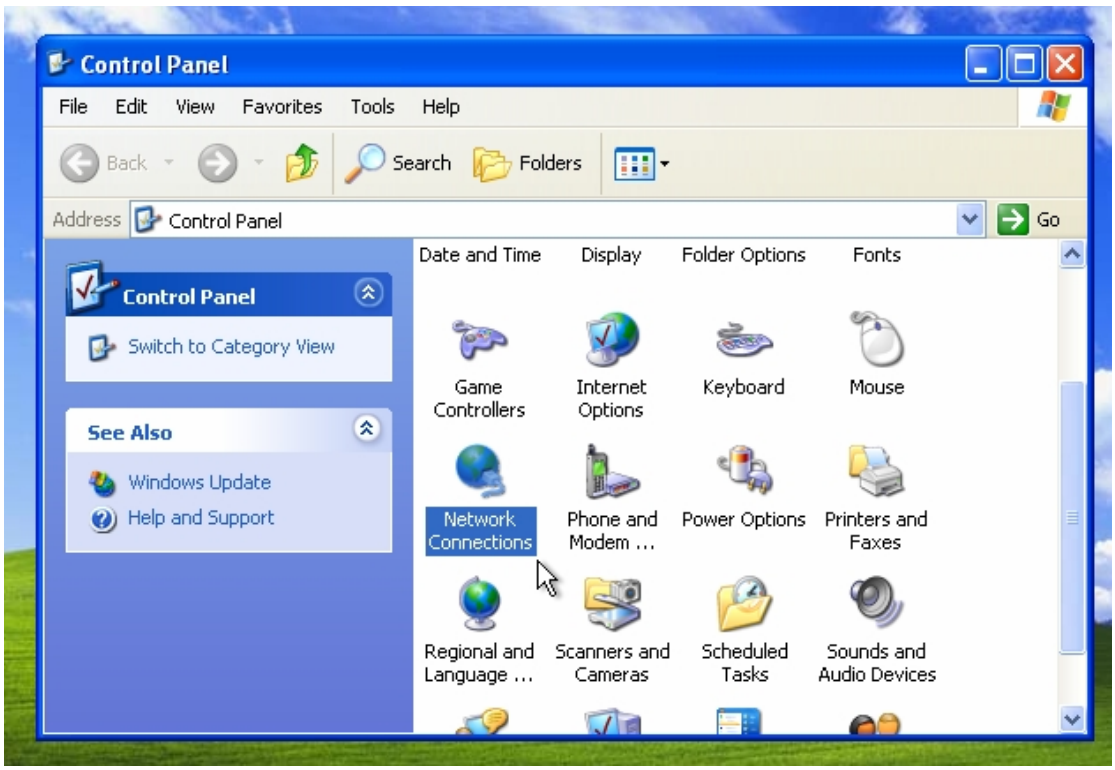

**در پنجرهٔ ظاهر شده عبارت ipconfig را تایپ کنید و کلید Enter را بزنید.**



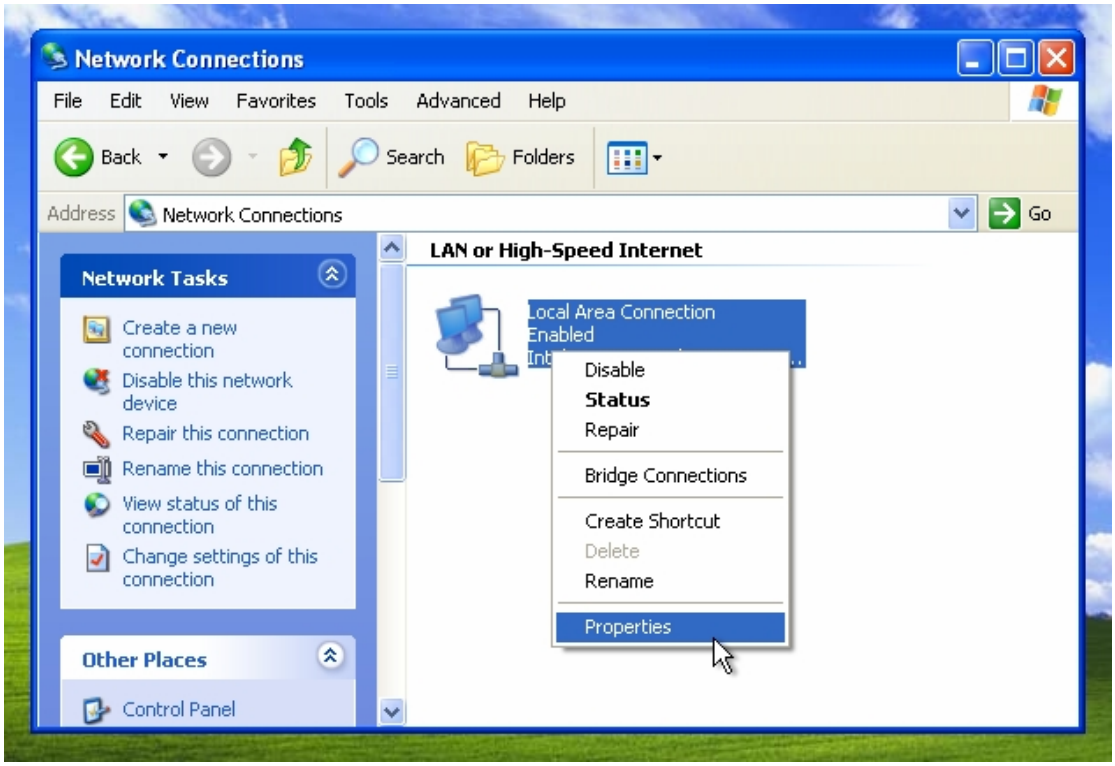



**عبارت نمایش داده شده در مقابل** IP Address**، IP کامپیوتر می‌باشد.**

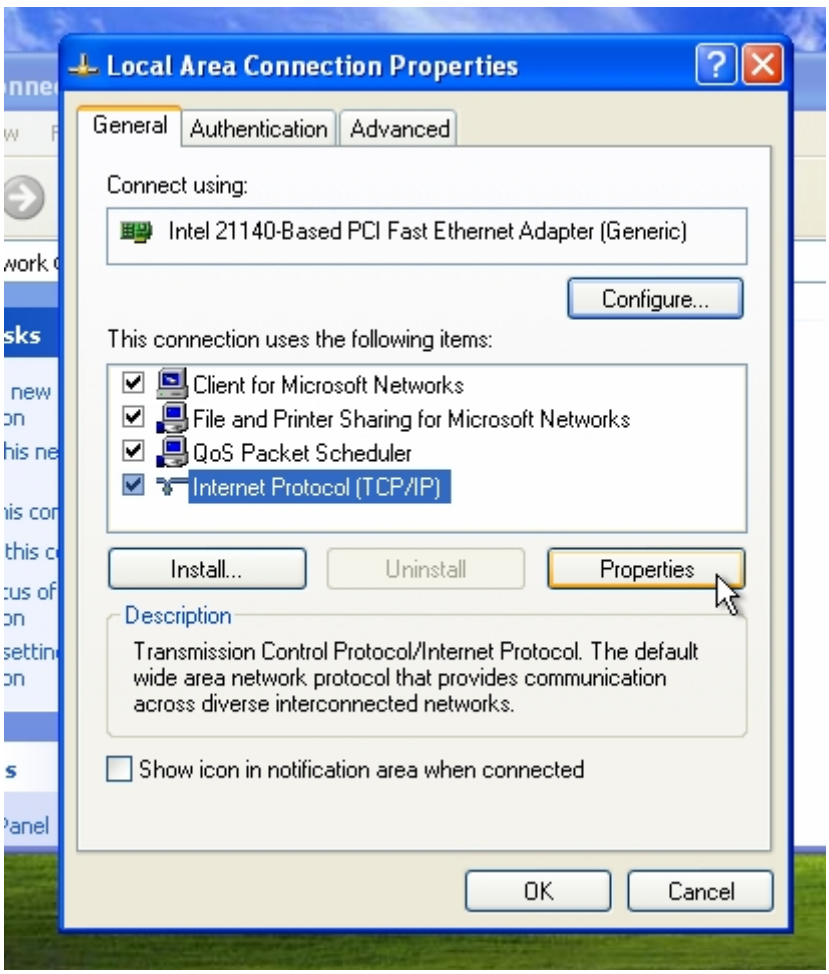
**در روش دوم، از منـــوی** Start **وارد** Control panel **شـــوید و علامـــت** Network connections **را انتخاب کنید.**



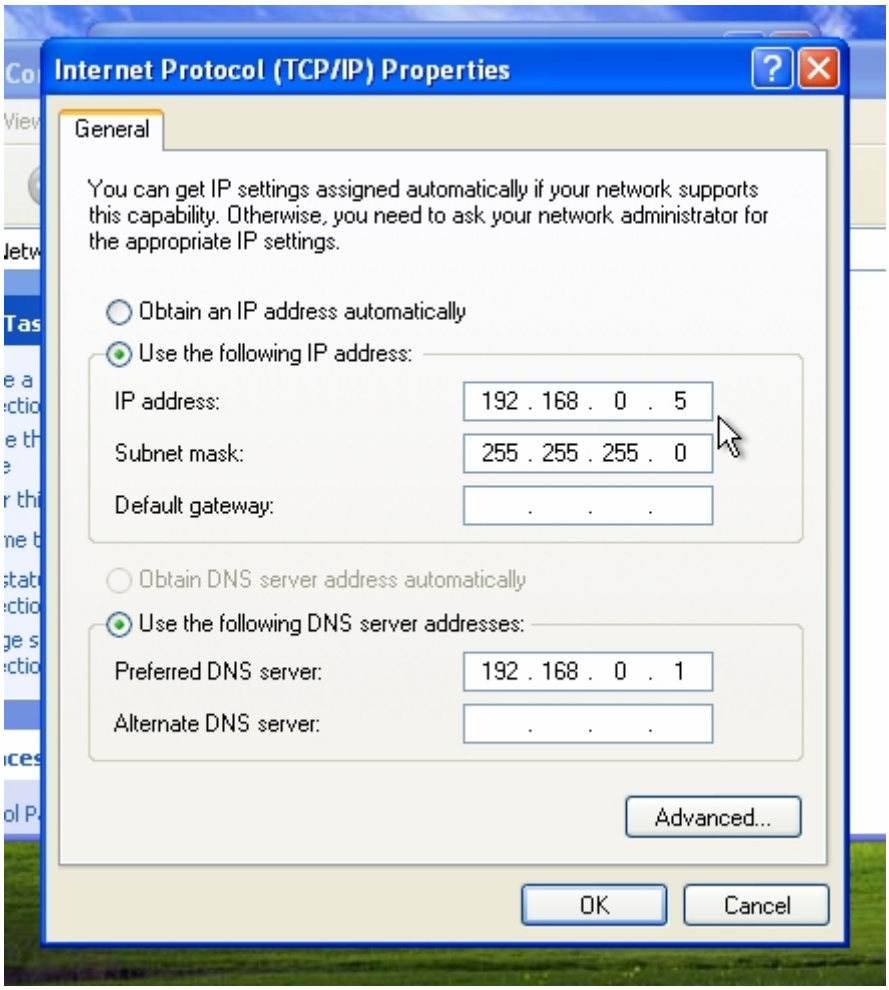

**سپس در پنجرهٔ ظاهر شده، بر روی علامت کارت شبکه، دکمهٔ سمت راست موس را بزنیـد و گزینهٔ** Properties **را انتخاب کنید.**




**در پنجرهٔ ظاهر شده، از لیست موجود، گزینهٔ Internet Protocol (TCP/IP) را انتخاب کنید و دکمهٔ Properties را کلیک کنید.**

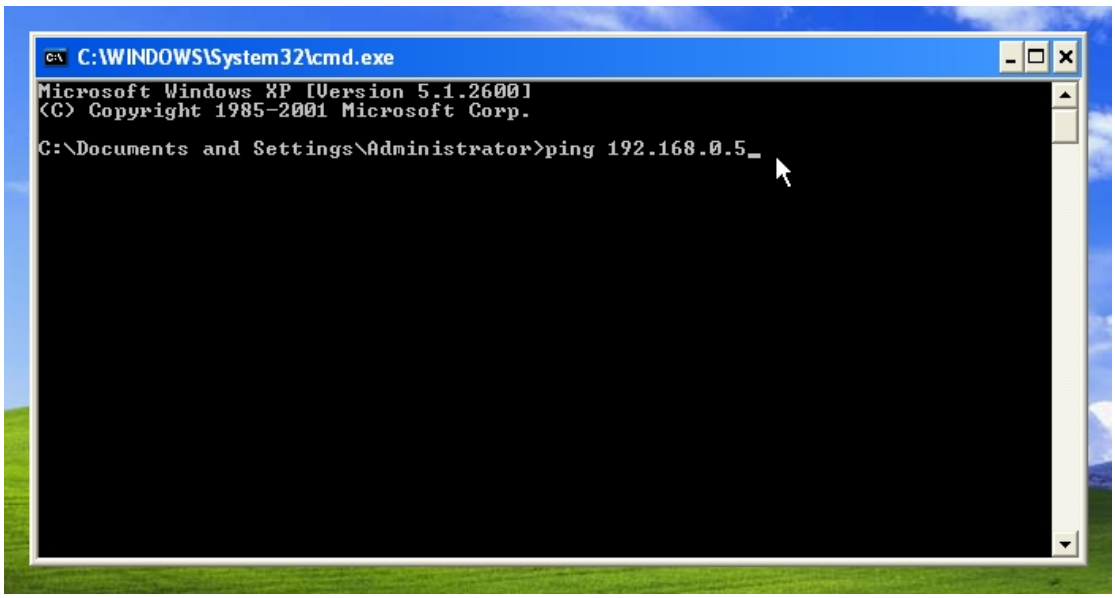


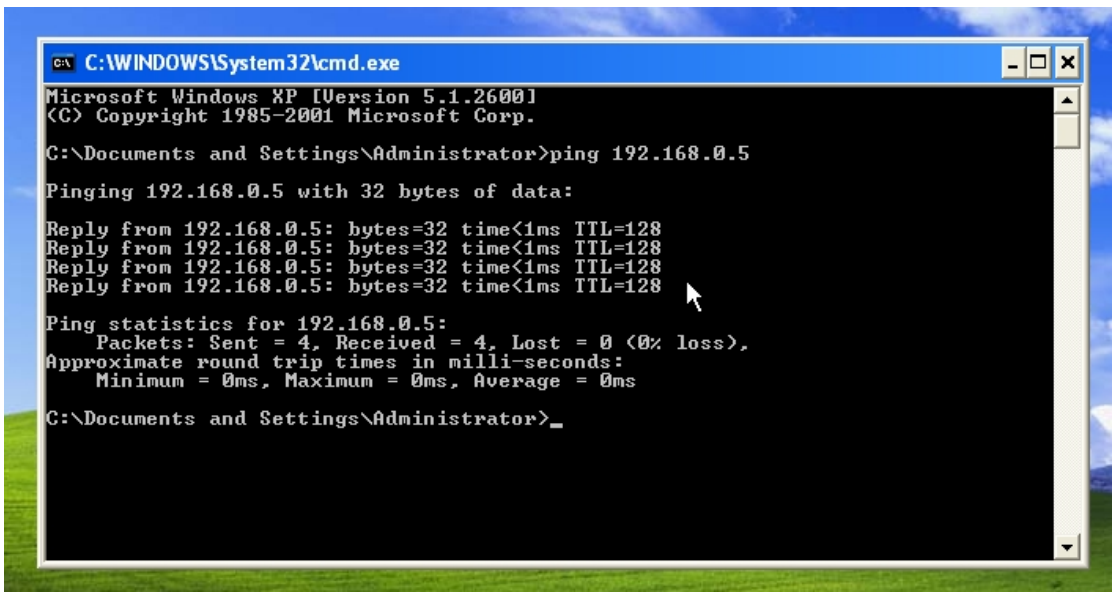
در پنجـرۀ بعـدی، اعـداد ذکـر شـده در روبـروی IP Address، نـشان دهنـدۀ IP کـامپیوتر می‌باشند.




در این پنجره با وارد کردن اعداد جدید، می‌توانید IP کامپیوتر خود را تغییر دهید. فقط بایـد توجه داشته باشید که این IP، نباید برای کامپیوتر دیگری اسـتفاده شـده باشـد. بـرای اعمـال تغییرات IP نیازی به Restart کردن کامپیوتر نیست.

به عنوان یک تمرین ساده، می‌توانید بر روی یک کامپیوتر دیگر در شبکه، گزینـۀ Run را از منوی Start انتخاب کند. سپس عبارت cmd را وارد کنیـد و کلیـد OK را انتخـاب کنیـد. در پنجرۀ ظاهر شـده، عبـارت "Ping xxxx" را وارد کنیـد (بجـای xxxx، IP کـامپیوتر خـود را تایپ کنید). سپس کلید Enter را بزنید.




**در صورتیکه ارتباطات شبکه مشکلی نداشته باشد، چهار پیغام از طرف کامپیوتر فعلی، به کامپیوتر شما فرستاده می‌شود و جواب دریافتی از کامپیوتر شما، نمایش داده می‌شود.**

**در تعویض IP کامپیوتر، نکات زیر را مد نظر داشته باشید :**

a. **جهت تعویض IP کامپیوتر، باید حتما Administrator و یا عضوی از گروه Administrators باشید.**

b. **در صورتیکه کامپیوتر در شبکه باشد، ممکن است سیاست‌های اعمال شده بر روی شبکه، از تغییر IP جلوگیری کند.**

- ***مفهوم Subnet Mask***

Subnet mask نیز، مانند IP از چهار عدد یک بایتی تشکیل شده است. پس اعداد تشکیل دهندهٔ Subnet mask نیز هرکدام بین صفر تا ۲۵۵ می‌باشند. هدف از subnet mask، تعیین دامنهٔ شبکه و یا تقسیم شبکه به چند شبکهٔ کوچکتر می‌باشد. در حقیقت ترکیب IP با Subnet mask، مشخص می‌کند که چه محدوده IP در داخل شبکه بکار رفته است. به عنوان مثال ترکیب زیر را در نظر بگیرید :


اعداد موجود در Subnet mask، یک به یک با اعداد موجود در IP، متناظر می‌باشند. عدد ۲۵۵ موجود در Subnet mask، نشاندهندهٔ ثابت بودن عدد متناظر آن در IP، در کل شبکه است. به عبارت دیگر، IP کلیهٔ کامپیوترهای موجود در شبکه در مثال بالا با اعداد 192.168.0 شروع می‌شوند. تنها عدد چهارم این IPها متغیر است. به قسمت‌هایی از IP که در شبکه ثابت است، Network ID و به قسمت‌هایی که در هر کامپیوتر متغیر است Host ID، می‌گویند.

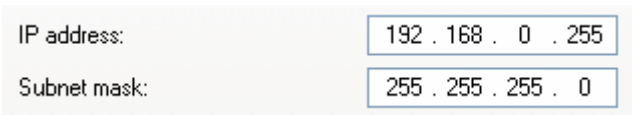
اگر عدد Host ID را به همراه اعداد متناظر آن در Subnet mask، تبدیل به باینری کنیم و با هم جمع نماییم، بیت‌های عدد بدست آمده نمی‌تواند همگی ۱ یا صفر باشد. در مثال بالا :

Host ID = 5 = 00000101 (binary)

0 = 00000000 (binary)

00000101 + 00000000 = 00000101

پس ترکیب IP فوق با Subnet mask آن درست است. ولی مثال زیر را در نظر بگیرید :



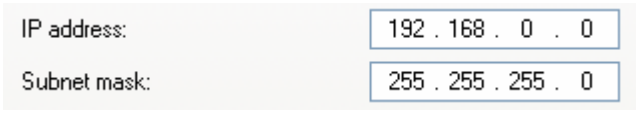

در این مثال :

Host ID = 255 = 11111111 (binary)

0 = 00000000 (binary)

11111111 + 00000000 = 11111111

بدلیل اینکه در جمع حاصل کلیهٔ بیت‌ها عدد ۱ می‌باشد، پس این IP صحیح نمی‌باشد. مثال بعدی را در نظر بگیرید :



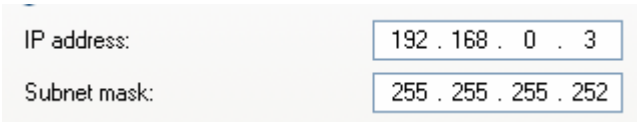

در این مثال :

Host ID = 0 = 00000000 (binary)

0 = 00000000 (binary)

00000000 + 00000000 = 00000000

بدلیل اینکه در این جمع کلیهٔ بیت‌ها عدد صفر می‌باشد، این IP صحیح نیست. مثال سوم :




در این مثال :

Host ID = 3 = 00000011 (binary)

252 = 11111100 (binary)

00000011 + 11111100 = 11111111

این مثال نیز بدلیل ۱ بودن کلیهٔ بیت‌های جمع حاصل غلط است.

پس جمع هر کدام از اعداد موجود در Host ID و عدد متناظر آن در Subnet mask، نمی‌تواند مساوی صفر یا مساوی ۲۵۵ یا بیشتر از ۲۵۵ باشد. به همین دلیل در مثال اول، ۲۵۴ کامپیوتر مجزا می‌تواند در شبکه موجود باشد. در مثال چهارم با فرض Subnet mask 255.255.255.252، تنها دو کامپیوتر با IPهای 192.168.0.1 و 192.168.0.2، می‌توانند در شبکه وجود داشته باشند.

شرط دیگر برای اعداد Subnet mask، ترتیب ۱های موجود در باینری آن‌ها می‌باشد. اولا تبدیل باینری هر کدام از اعداد موجود در Subnet mask باید با ۱ شروع شده باشد. پس کوچکترین عدد ممکن برای Subnet mask، عدد ۱۲۸ (10000000 binary) است. دوما کلیهٔ ۱ های بعدی باید متصل به ۱ اول باشند. یعنی عدد ۱۶۰ (10100000 binary) غلط و عدد ۱۹۲ (11000000 binary) صحیح می‌باشد.

هنگام برقراری ارتباط، کامپیوتر به ترکیب IP و Subnet mask خود نگاه می‌کند. از این ترکیب، کامپیوترهایی را که در شبکهٔ خود وجود دارند تشخیص داده و با آن‌ها مستقیما ارتباط برقرار می‌کند.

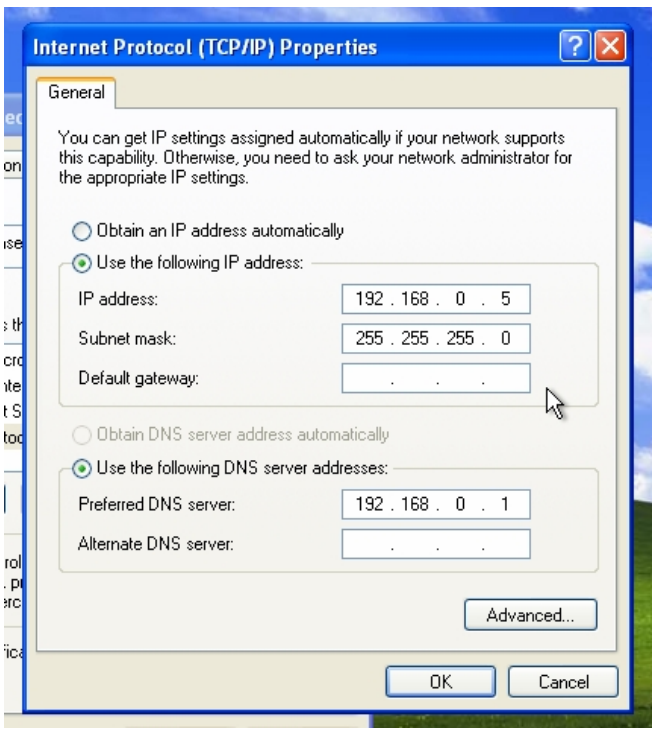
- ***مفهوم Gateway***

در بخش مربوط به IP ، توضیح داده شد که کامپیوتر از ترکیب IP و Subnet mask خود، می‌تواند تشخیص دهد که چه IPهایی در شبکهٔ خود وجود دارد. به عنوان مثال، هنگامیکه کامپیوتری با مشخصات زیر بخواهد با کامپیوتری با IP، 192.168.0.18 ارتباط برقرار کند،


می‌تواند تشخیص دهد که این کامپیوتر در شبکهٔ خود وجود دارد. پس مستقیما با آن کامپیوتر ارتباط برقرار می‌کند. حال اگر همین کامپیوتر، بخواهد با کامپیوتری که IP آن 192.168.5.18 است ارتباط برقرار کند چه اتفاقی می‌افتد؟

کامپیوتر این IP را با IP و Subnet mask خود مقایسه می‌کند. این IP در شبکهٔ تعریف شده برای این کامپیوتر وجود ندارد. پس این کامپیوتر نمی‌تواند مستقیما با آن ارتباط برقرار کند. کامپیوتر مجبور است برای برقراری ارتباط از یک واسطه بنام Gateway استفاده کند. در واقع، کامپیوتر این درخواست را برای gateway فرستاده، و gateway بجای کامپیوتر این ارتباط را برقرار می‌کند.

هنگام تعریف IP ، مکانی برای تعریف gateway IP وجود دارد :



در شکل بالا، قسمت Default gateway، آدرس gateway شبکه وارد می‌شود. این Gateway، می‌تواند یک کامپیوتر و یا یک router باشد.

IPای که برای gateway وارد می‌شود، باید از جنس IP خود کامپیوتر باشد. یعنی باید در همان شبکه‌ای باشد، که کامپیوتر در آن قرار گرفته، تا کامپیوتر بتواند مستقیم با آن ارتباط برقرار کند.

- ***تنظیمات DNS***

استفاده از IP، هنگام برقراری ارتباط بین دو کامپیوتر، مشکل است. مخصوصا در شبکه‌هایی که تعداد کامپیوترهای آن‌ها زیاد است، بخاطر سپردن IPهای کامپیوترهای مختلف، کار ساده‌ای نیست. معمولا به خاطر سپردن اسامی، راحتتر از IP است. به همین دلیل در شبکه از سرویسی بنام DNS استفاده می‌شود که این سرویس، وظیفهٔ تبدیل اسامی به IP را در شبکه دارد. این سرویس، معمولا بر روی یک کامپیوتر مجزا در شبکه وجود دارد. هنگامیکه کامپیوتر ما بخواهد، مثلا با کامپیوتری بنام "xp2" ارتباط برقرار کند، ابتدا این نام را به کامپیوتری که سرویس DNS بر روی آن وجود دارد فرستاده و از آن IP این کامپیوتر را دریافت می‌کند. سایر مراحل مانند قبل انجام می‌گیرد.

در پنجرهٔ تعریف IP، دو مکان برای تعریف دو DNS مجزا، تحت عنوان Preferred DNS Server و Alternate DNS Server وجود دارد.

# شبکه‌های مبتنی بر Domain

شبکه‌های مبتنی بر Domain، به شبکه‌هایی گفته می‌شود که در آن کلیهٔ کامپیوترها عضوی از یک Domain خاص می‌باشند. در این نوع شبکه‌ها، کنترل کلیهٔ کامپیوترها بصورت مرکزی و توسط کامپیوتری که به آن Domain controller گفته می‌شود، انجام می‌شود. یک Domain، با راه‌اندازی اولین Domain Controller در شبکه بوجود می‌آید. در شبکه‌های ویندوز ۲۰۰۳، به کامپیوتری Domain controller گفته می‌شود که بر روی آن سرویس Active directory نصب شده باشد.

برخلاف شبکه‌های workgroupای، در شبکه‌های Domainای، کلیهٔ کارهای مدیریتی مانند تعریف کاربر، تعریف دسترسی و غیره بصورت مرکزی و متمرکز انجام می‌گیرد.

- ***سرویس Active Directory***

سرویس دایرکتوری، یک ساختار درختی است که وظیفهٔ نگهداری اطلاعات در مورد اجزا مختلف شبکه را دارا می‌باشد. در سیستم‌عامل‌های ویندوز ۲۰۰۰ سرور به بعد، نام این سرویس، Active directory گذاشته شده است.

شرکت مایکروسافت با تغییراتی که بر روی سرویس دایرکتوری، سرورهای خود بوجود آورده است، امکان تمرکز بیشتر اطلاعات شبکه را بوجود آورده است.

در حقیقت، Active directory، یک بانک اطلاعاتی است که از ۳ قسمت تشکیل شده است: Domain، که اطلاعات مربوط به کاربران، کامپیوترها، تقسیم‌بندی‌ها و غیره را نگهداری می‌کند، schema، که اطلاعات مربوط به اشیا موجود در Domain و صفات هر کدام از آن‌ها را نگهداری می‌کند و configuration که اطلاعات مربوط به تنظیمات مختلف Active directory را نگهداری می‌کند.

- **کاربرد**

همانطور که گفته شد، سرویس Active directory، جهت نگهداری اطلاعات مختلف شبکه، بصورت متمرکز استفاده می‌شود. این اطلاعات می‌تواند شامل اطلاعات مختلف کاربران موجود در شبکه مانند رمز، نام و آدرس آن‌ها، کامپیوترها و سیاست‌هایی که باید در مورد آن‌ها اعمال شود و غیره باشد.

برای ایجاد یک Domain، راه‌اندازی سرویس Active directory ضروری است.

همچنین Active directory، یک محیط متمرکز را جهت مدیریت شبکه، بوجود می‌آورد. در این محیط، کلیهٔ کاربران و کامپیوترهای موجود در شبکه، از یک مکان قابل مدیریت هستند.

- **پیش‌نیازهای راه‌اندازی سرویس Active Directory**

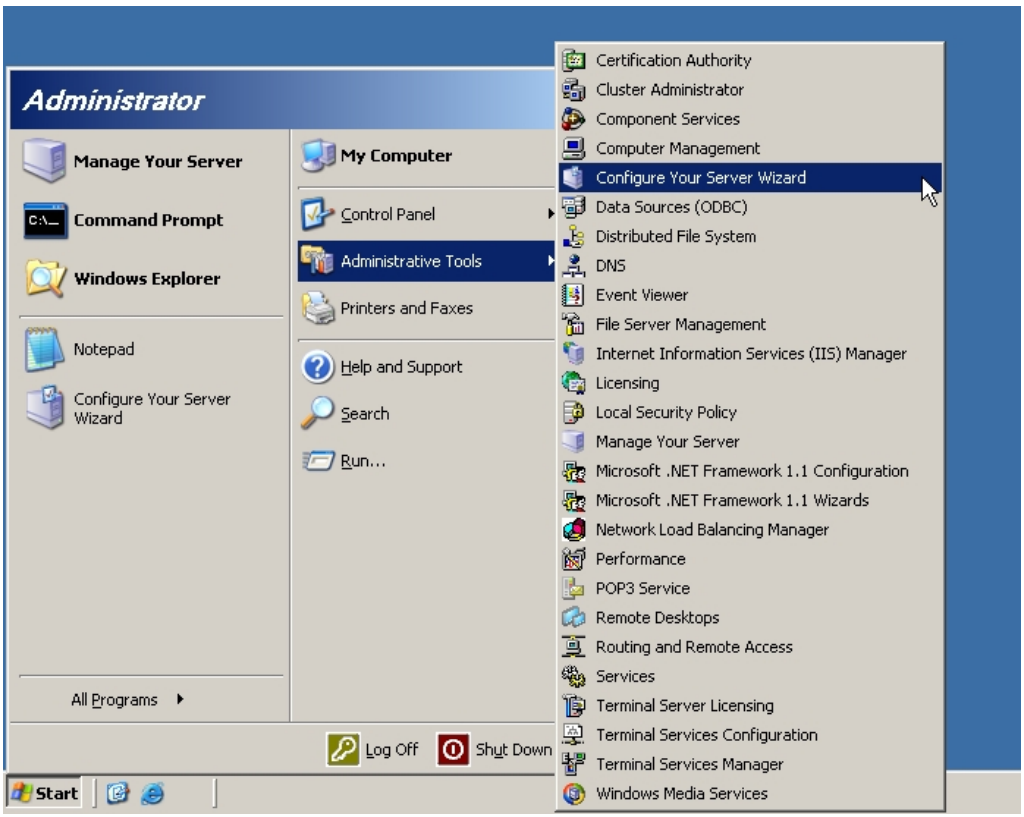
سرویس Active directory، فقط بر روی ویندوز سرور نصب می‌شود. جهت نصب این سرویس، احتیاج به یک IP استاتیک می‌باشد. در ضمن سرویس DNS باید بر روی شبکه موجود باشد ( در غیر اینصورت، بطور اتوماتیک نصب خواهد شد).

باید توجه داشت که برای هر domain، تنها یک domain controller می‌تواند وجود داشته باشد. سرویس Active directory، فقط بر روی پارتیشن‌های NTFS نصب می‌شود.

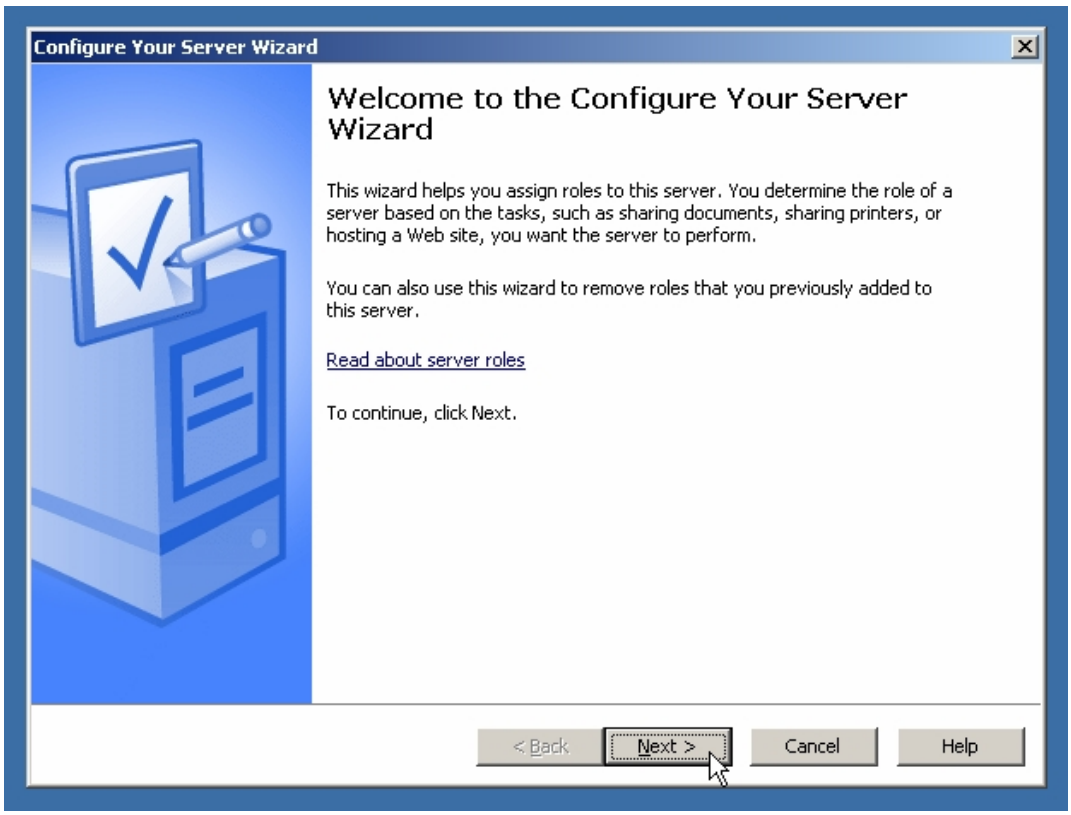
## نحوهٔ راه‌اندازی سرویس Active Directory

جهت نصب سرویس Active directory، روشهای مختلفی وجود دارد. در روش اول، با استفاده از Configure your server wizard، سرویس بر روی سرور نصب می‌شود:

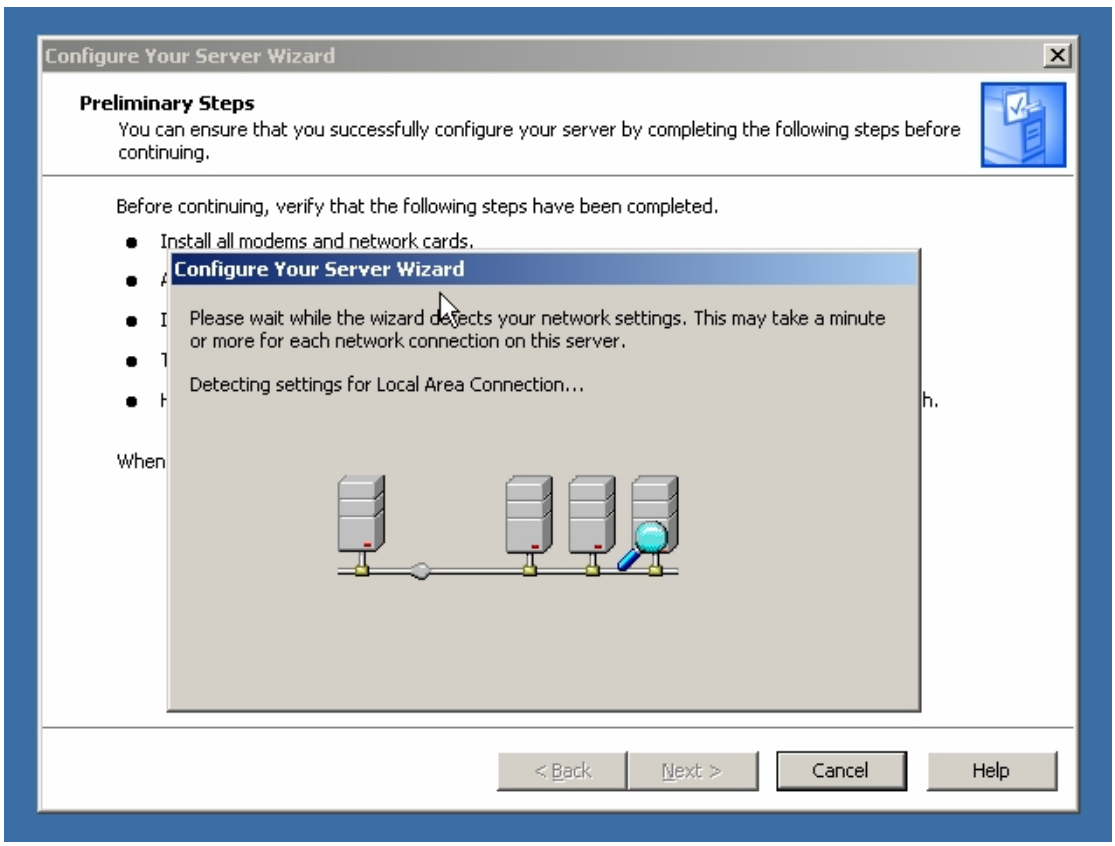
از منوی Start، بر روی گزینهٔ Administrative Tools رفته و گزینهٔ Configure Your Server Wizard را انتخاب کنید. منوی Administrative tools را می‌توانید در داخل Control panel نیز پیدا کنید.



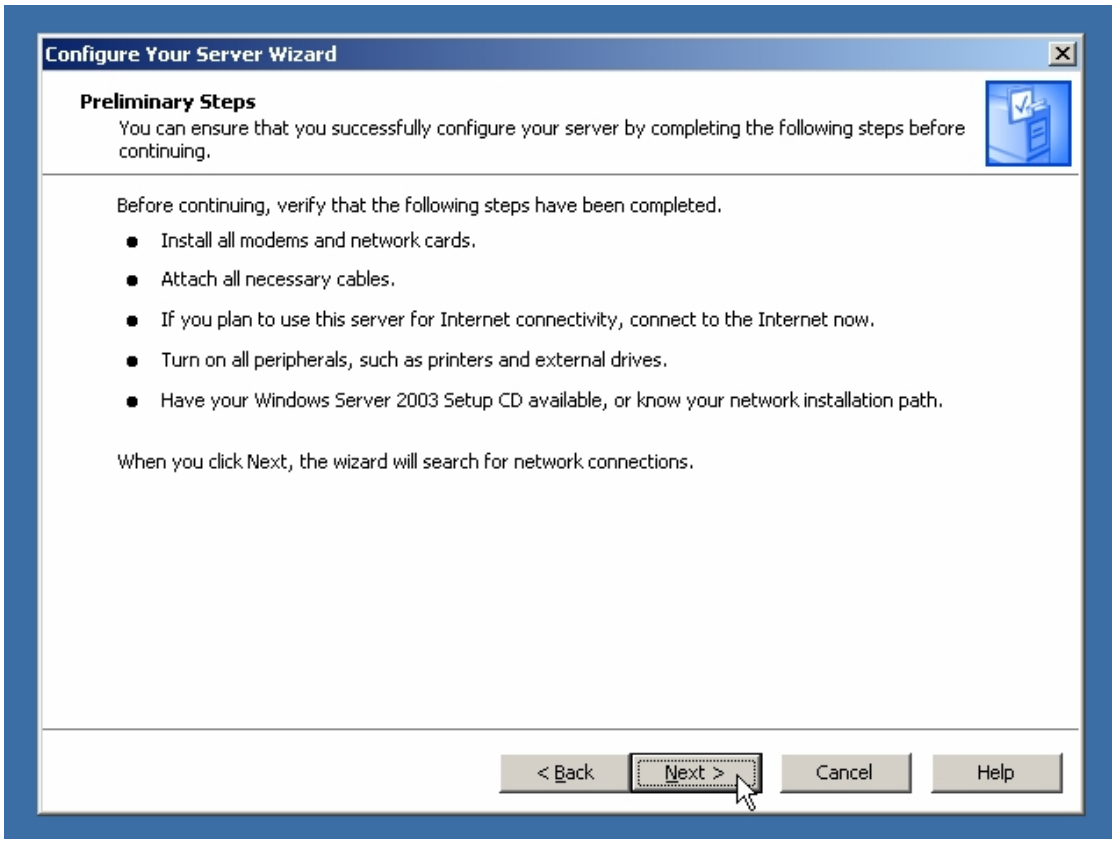

سپس از پنجرهٔ ظاهر شده گزینهٔ Next را انتخاب کنید.



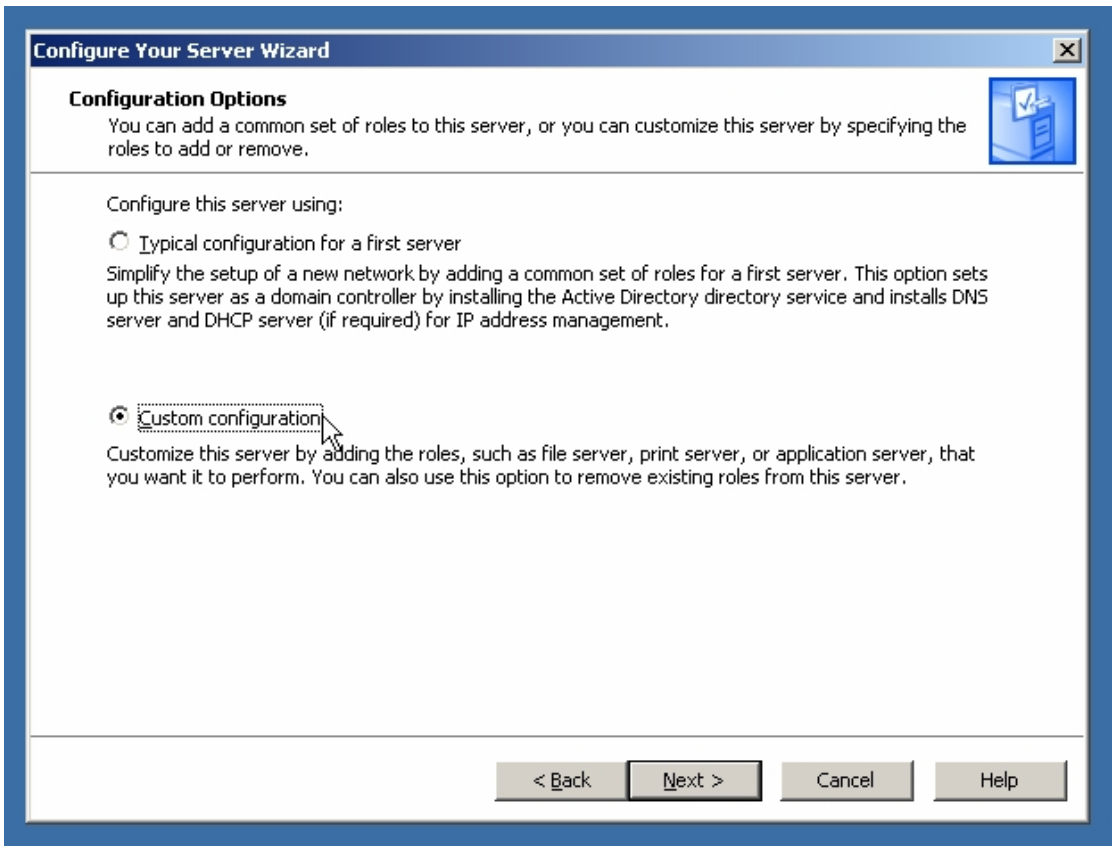

پنجره‌ای ظاهر شده و ترکیب فعلی شبکه بررسی می‌شود. در این قسمت وجـود یـا عـدم وجود یک Domain Controller در شبکه نیز تعیین می‌شود.



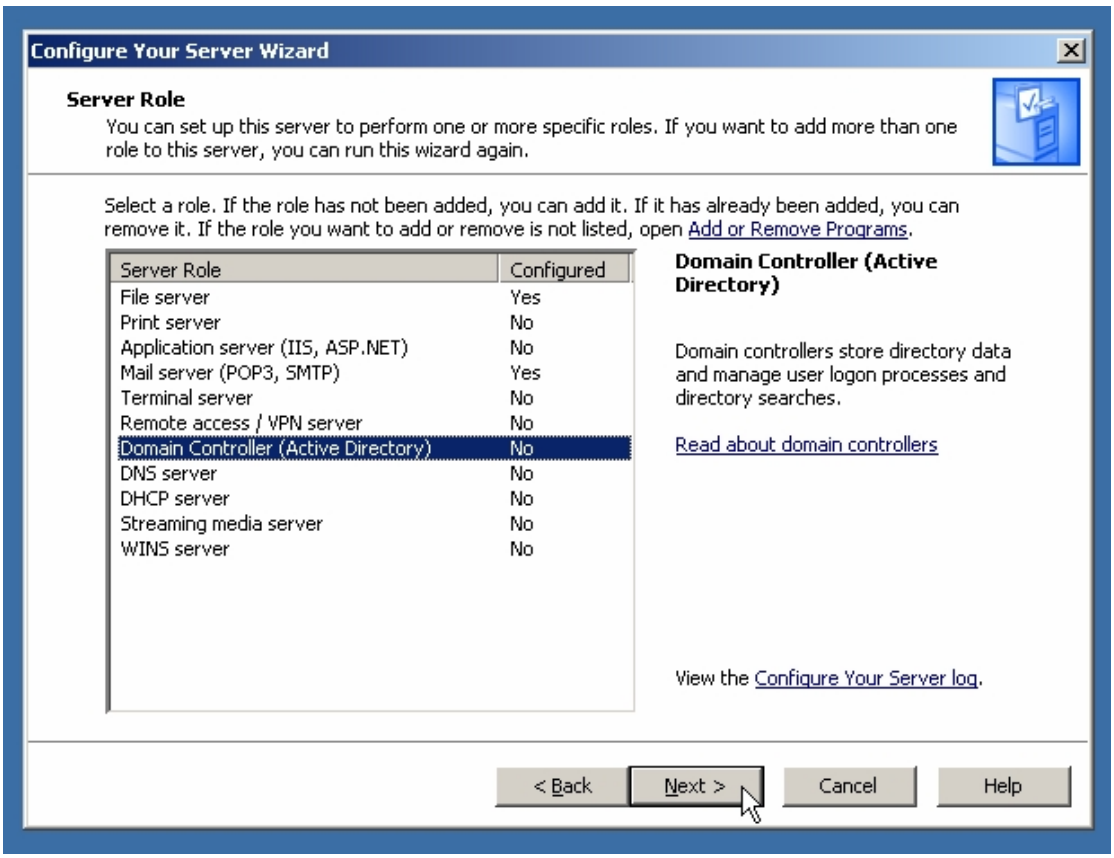
در پنجرهٔ بعدی، توصیه‌هایی در مورد نصب کامل کلیهٔ سخت‌افزارهای کامپیوتر می‌شود.
در این قسمت نیز گزینهٔ Next را انتخاب کنید.



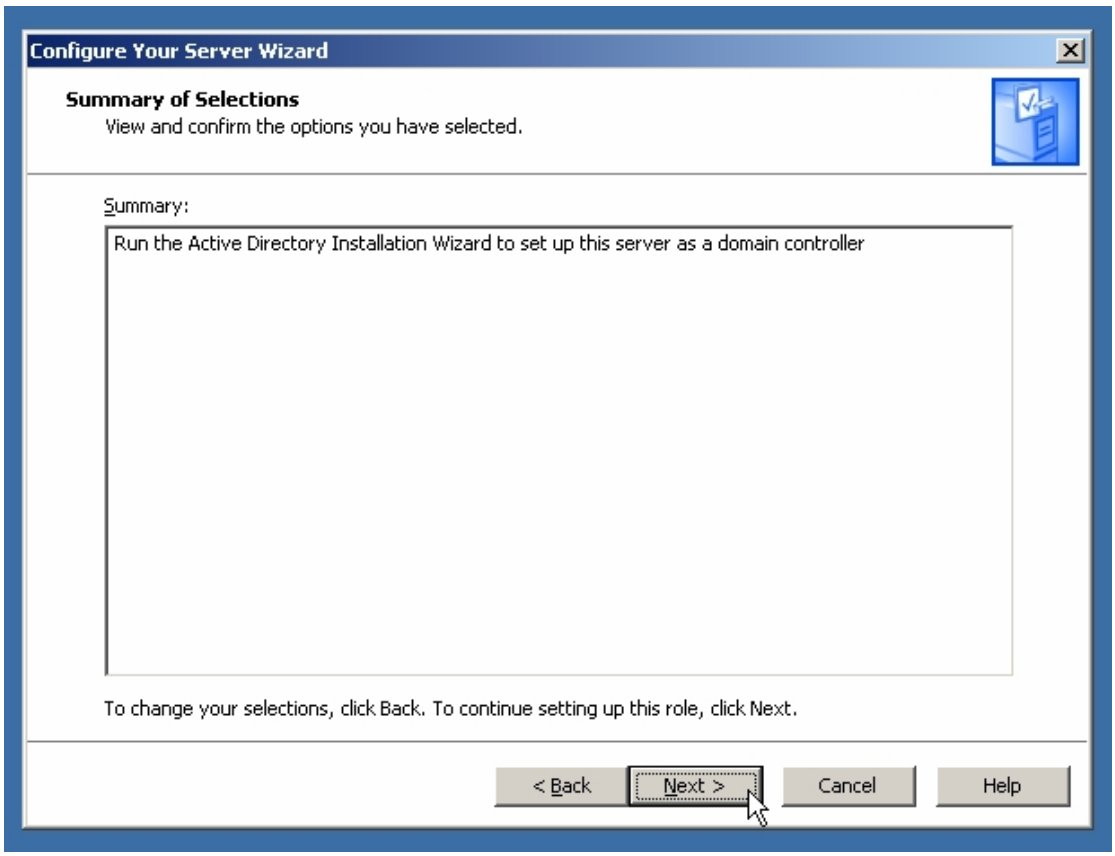

سپس گزینهٔ Custom configuration را انتخاب کنید و دکمهٔ Next را بزنید.




**در این پنجره، می‌توان وظـایف مختلفـی را بـرای کـامپیوتر (سـرور خـود) تعریـف کـرد. وظیفه‌ای که ما می‌خواهیم بر عهدهٔ سرور خود قرار دهیم، وظیفهٔ** Domain controller **شبکه است. پس این گزینه را از داخل لیست انتخاب کنید و دکمهٔ** Next **را بزنید.**

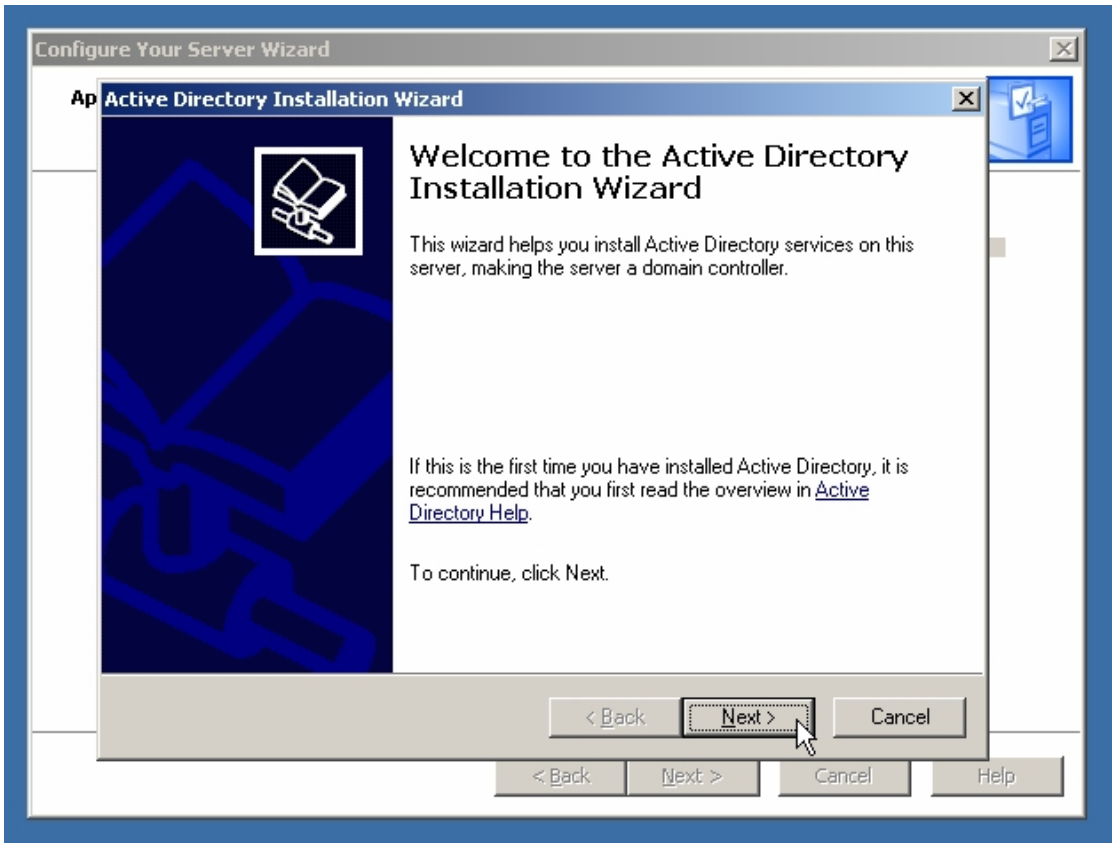



**در پنجرهٔ بعدی نیز که خلاصه‌ای از اعمالی که بایـد انجـام بگیـرد را آورده اسـت، دکمـهٔ Next را بزنید.**

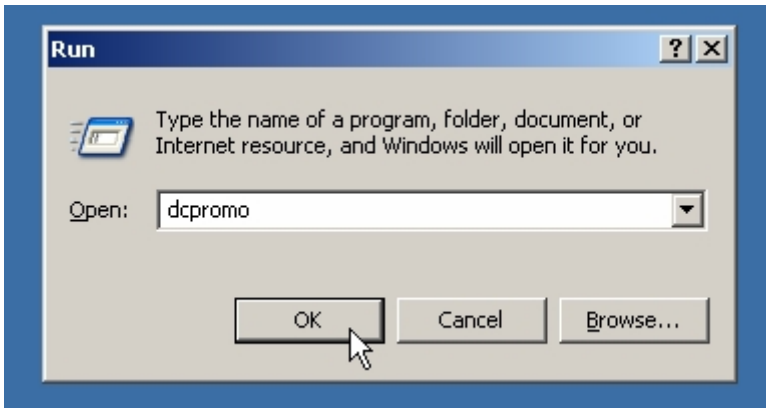



**پس از زدن دکمهٔ Next، مراحل نصب Active directory بر روی سرور آغاز می‌شود.**

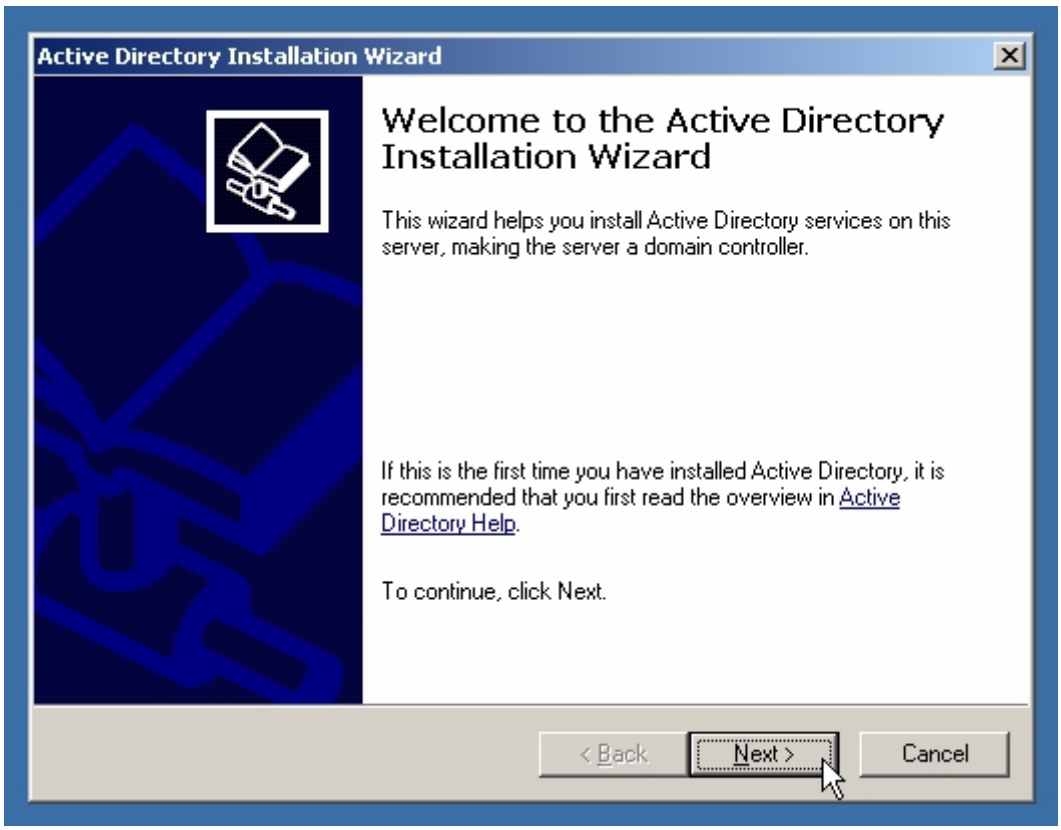
**این مراحل در قسمت‌های بعدی توضیح داده می‌شود.**



در روش دوم، از منوی Start گزینهٔ Run را انتخاب کنید. سپس کلمهٔ dcpromo را تایپ کرده، دکمهٔ Ok را بزنید.

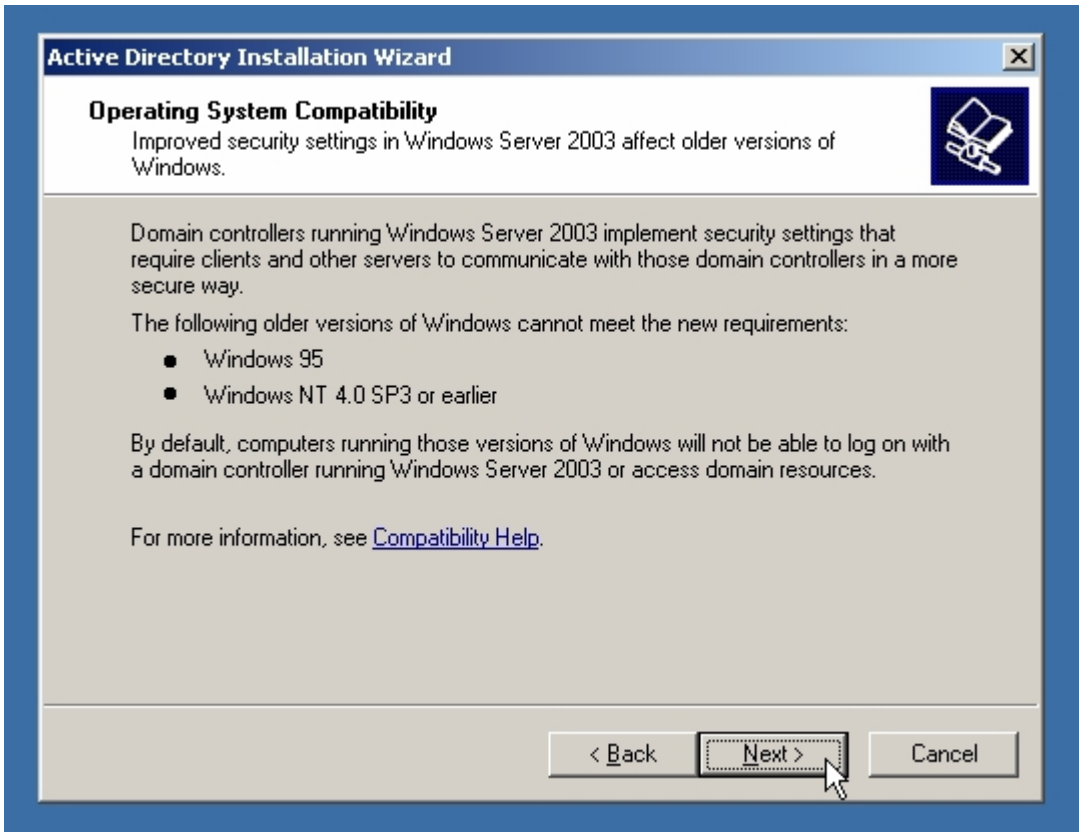



مانند روش اول، مراحل نصب Active directory شروع می‌شود.




- **نصب سرویس Active Directory**

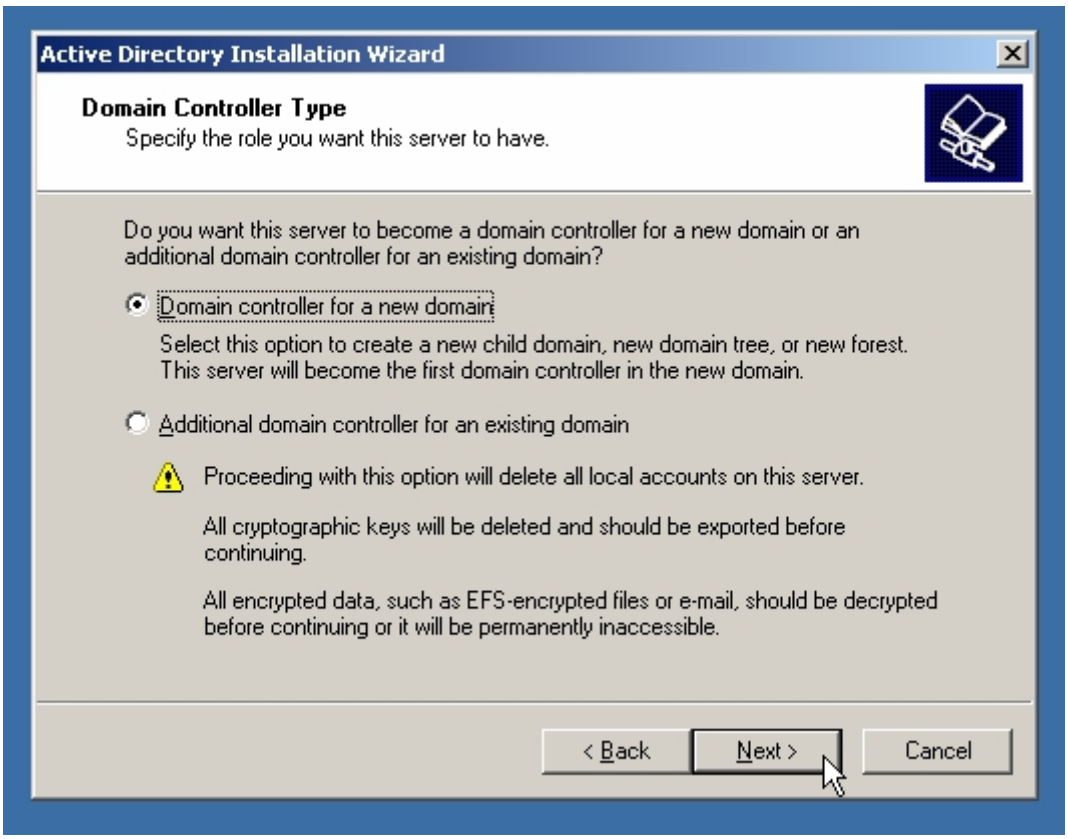
پس از فشار دادن دکمهٔ Next پنجرهٔ زیر ظاهر می‌شود. در این پنجره بر این نکته تاکید می‌شود که کامپیوترهایی که دارای سیستم‌عامل‌های windows 95 و windows NT 4 با service pack 3 یا قدیمی‌تر هستند، نمی‌توانند عضوی از شبکه‌های ویندوز ۲۰۰۳ باشند. دلیل این امر، نوع تنظیمات حفاظتیی است که در سرورهای ۲۰۰۳ وجود دارند و با نسخه‌های قدیمی ویندوز سازگار نیست.




**نخستین سوالی که هنگام نصب** Active directory **پرسیده می‌شود، نحوهٔ عملکـرد ایـن سرور در شبکه است. سرور فعلی می‌تواند خود یـک** Domain controller **بـرای یـک** Domain **جدید باشد، یا اینکه می‌تواند به عنـوان یـک** Domain controller **پـشتیبان برای یک** Domain **موجود، عمل کند.**

**با توجه به اینکه ما می‌خواهیم یک** Domain **جدید ایجاد کنـیم، گزینـهٔ اول** (Domain controller for a new domain) **را انتخاب می‌کنیم.**

**گزینهٔ** Additional domain controller for an existing domain**، این اجازه را به ما می‌دهد که سرورهایی را به عنوان پشتیبان برای** Domain **ای که از قبل موجود اسـت تعریف کنیم. در صورت از کار افتادن** Domain controller**، این سرور بطـور خودکـار وظیفهٔ سرویس دهی به شبکه را بعهده می‌گیرد.**



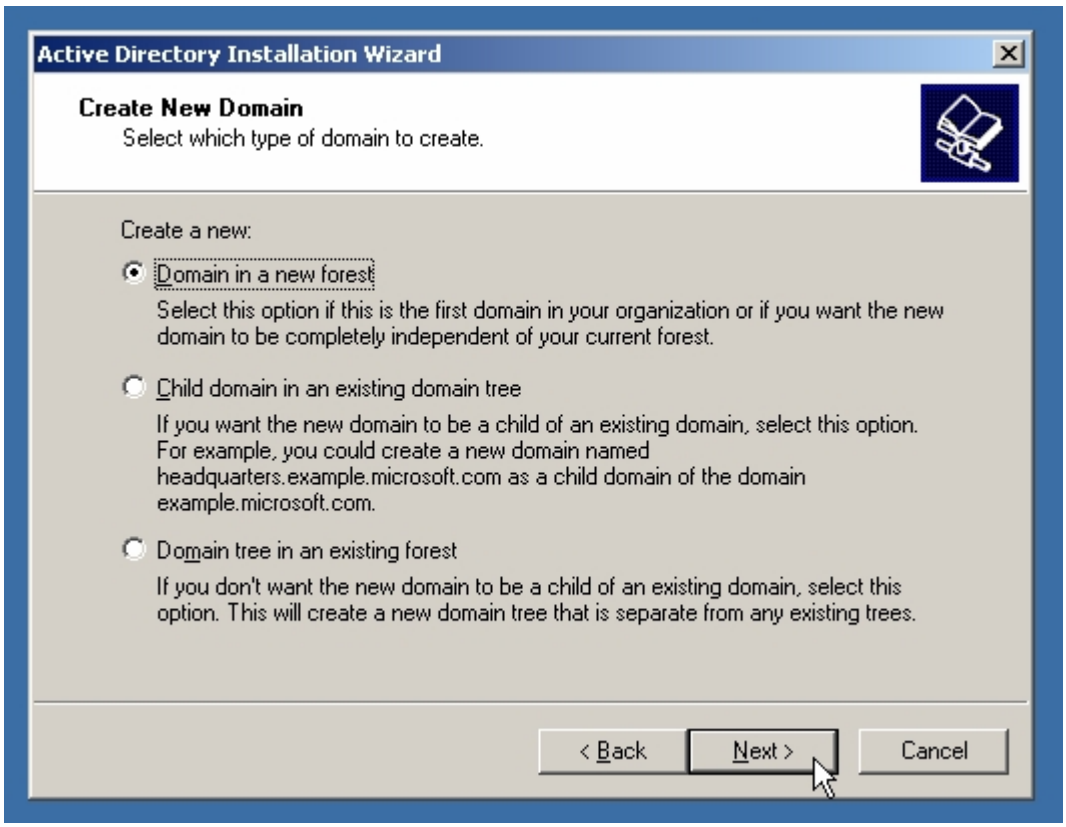

Domain جدید ما می‌تواند به سه صورت وجود داشته باشد. این Domain می‌تواند بطور کاملا مستقل ایجاد شود و به همین صورت کاملا مستقل فعالیت نماید.

در حالتی دیگر ، این Domain می‌تواند به زیر مجموعهٔ Domain دیگری که Domain پدر نامیده می‌شود، متصل شود و به عنوان یک فرزند در این Domain عمل نماید. مثلا اگر نام Domain ما Mail باشد و نام Domain پدر Rahmatizadeh.com باشد با انتخاب این گزینه، نام Domain ما Mail.Rahmatizadeh.com خواهد شد. جهت انتخاب این گزینه، Domain پدر باید از قبل وجود داشته باشد.

گزینهٔ سوم، سرور ما را تبدیل به یک Domain controller پدر که به آن می‌توانند، Domainهای دیگر، متصل شوند، می‌کند.

در صورتیکه سرور ما تنها domain controller موجود در شبکه باشد، باید گزینهٔ اول را انتخاب کنیم.

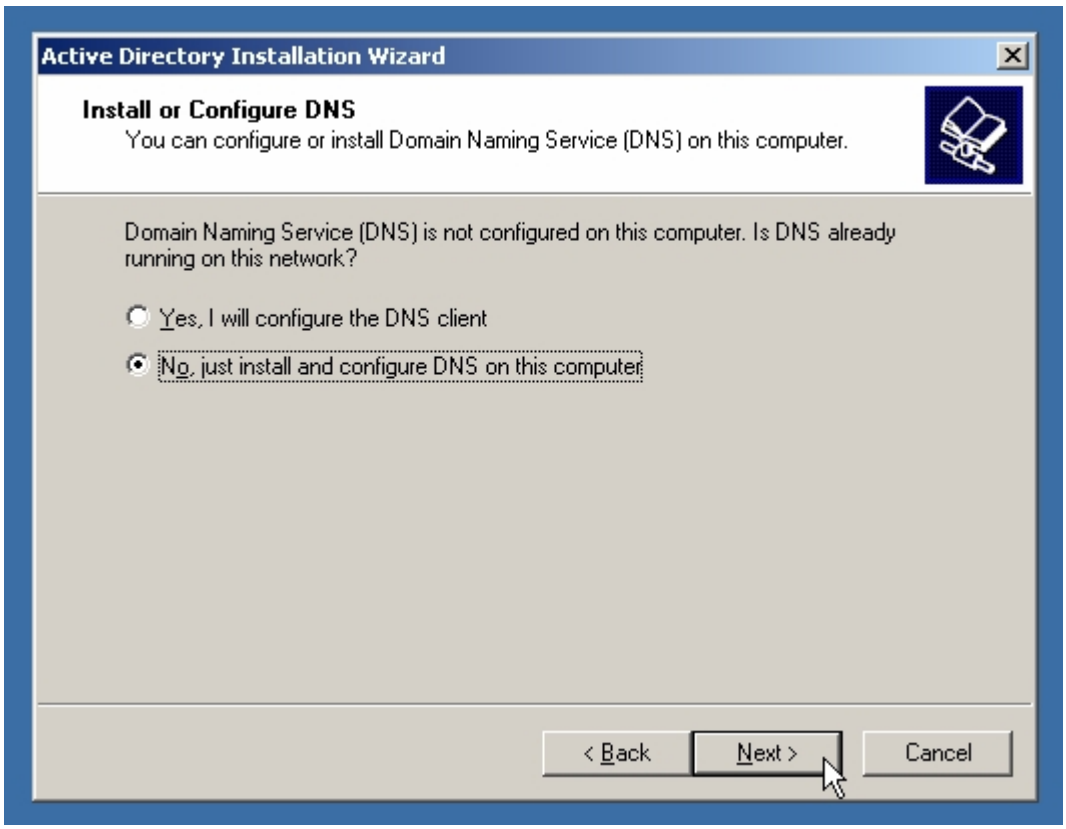
در این کلاس، ما به یک Domain کاملا مجزا نیاز داریم. به همین دلیل، گزینهٔ اول را که پیش‌فرض نیز می‌باشد انتخاب کرده و دکمهٔ Next را می‌زنیم.



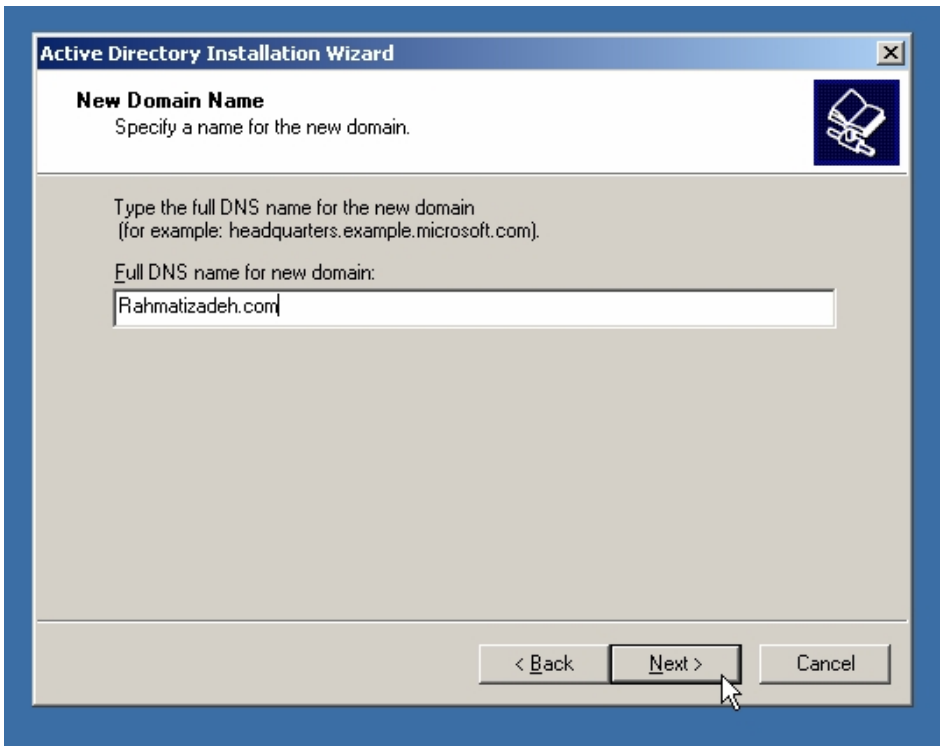

**همانطور که در ابتدای جزوه گفته شد، لازمهٔ داشتن سرویس Active directory، فعال بودن سرویس DNS در شبکه است. به همین دلیل در مرحلهٔ بعدی این سوال پرسیده می‌شود که آیا سرویس DNS در شبکهٔ ما وجود دارد یا نه. در صورتیکه این سرویس در شبکه وجود داشته باشد، گزینهٔ اول و در غیر اینصورت گزینهٔ دوم را باید انتخاب کنیم.**

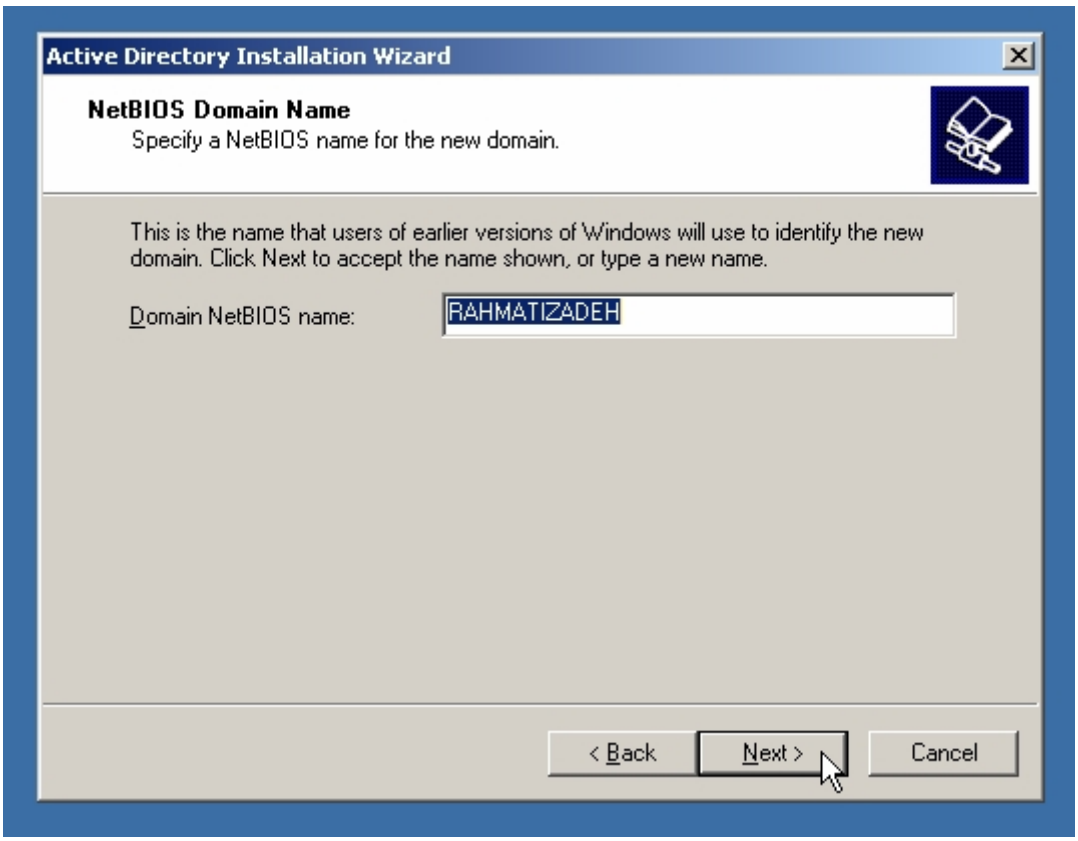
**گزینهٔ دوم، سرویس DNS را بر روی سرور ما نصب و راه‌اندازی می‌کند.**

**در این کلاس نیز با توجه به اینکه این سرور اولین سروری است که در شبکه راه‌اندازی می‌شود، گزینهٔ دوم را انتخاب می‌کنیم و دکمهٔ Next را می‌زنیم.**

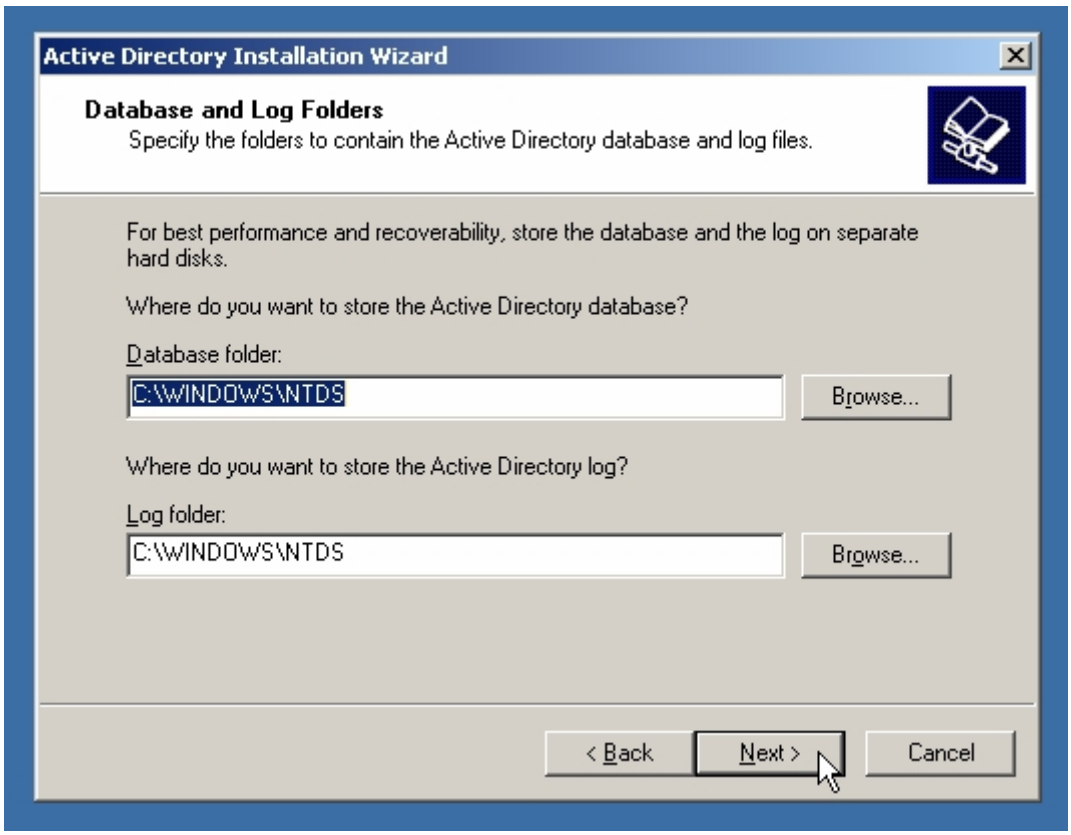



**در مرحلهٔ بعدی نام Domain از ما خواسته می‌شود. این نام می‌تواند یک نـام ثبـت شـده در اینترنت و یا غیره باشد. در پنجرهٔ اول نام کامل که شامل پسوند نیـز مـی‌باشـد را وارد می‌کنیم و در پنجرهٔ دوم، نام را بدون هیچ پسوند وارد می‌کنیم. دومین نام جهت اسـتفاده در سیستم‌عامل‌های قدیمی مانند windows 98 می‌باشد.**

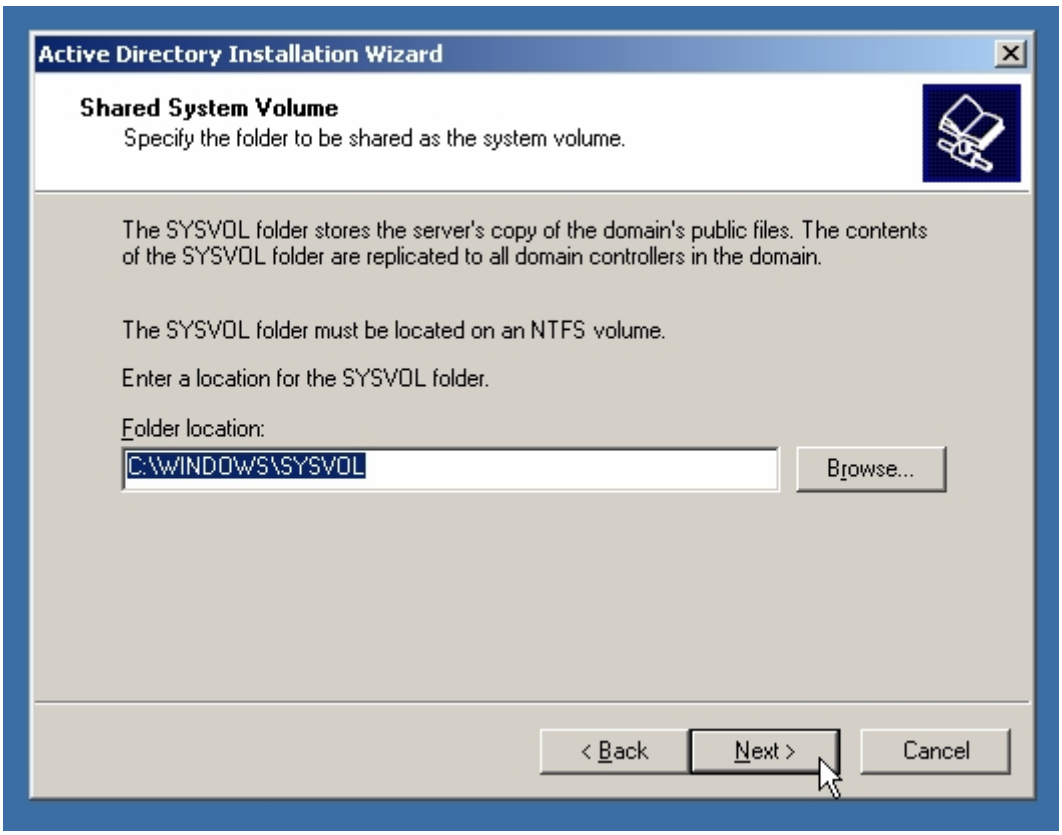





**سپس مسیری را که در آن فایل‌های بانک** Active directory **قرار می‌گیرد را مشخص می‌کنیم. در این مثال مسیر پیشنهادی را انتخاب کنید.**



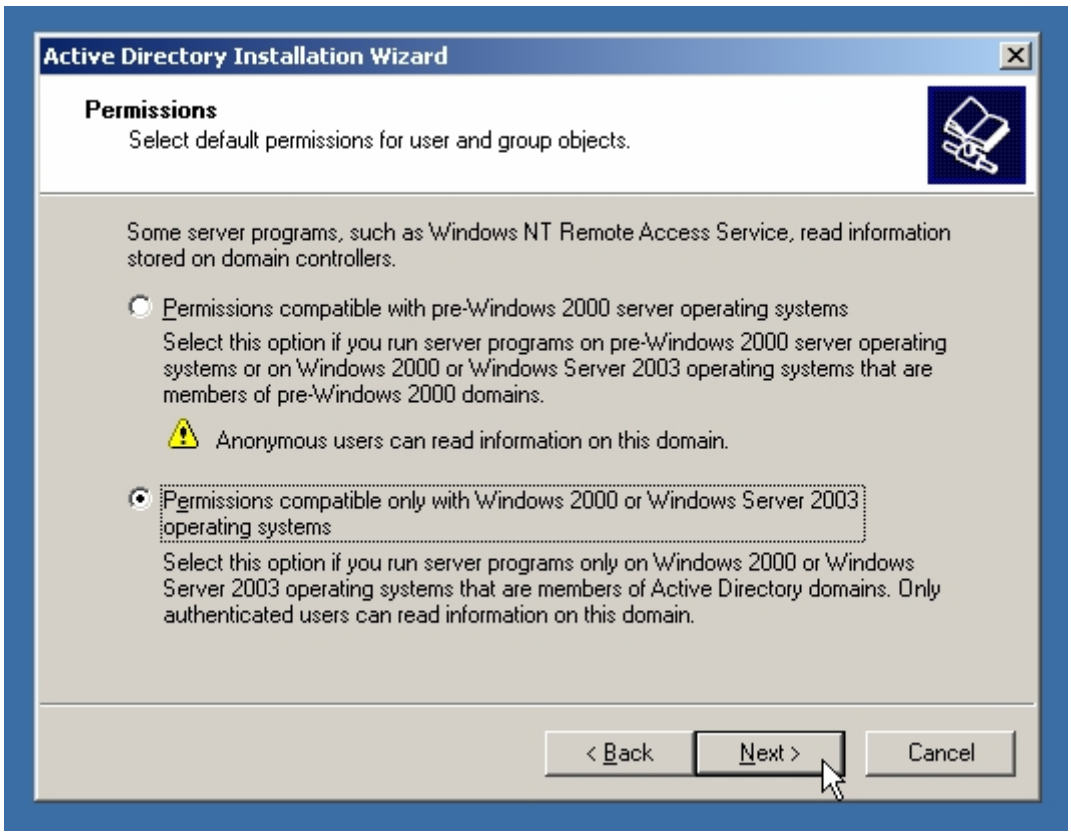
در هر domain controller، شاخه‌ای وجود دارد که اطلاعات عمومی شبکه بر روی آن قرار می‌گیرد. این شاخه در شبکه به اشتراک گذاشته می‌شود و اطلاعات موجود بـر روی آن، بطور اتوماتیک بر روی domain controllerهای دیگر، تکثیر می‌شود. مـسیر ایـن شاخه در این قسمت پرسیده می‌شود. این شاخه باید بر روی NTFS ساخته شود.




رکوردهـایی کـه در Active directory سـاخته مـی‌شـوند، بایـد قابـل خوانـدن توسـط برنامه‌های مختلف باشند. در نسخه‌های قدیمی ویندوز سرور مانند NT 4، کاربران بدون در نظر گرفتن دسترسی‌های تعیین شده، می‌توانستند به اطلاعات موجـود در directory دسترسی داشته باشند. در سرورهای ۲۰۰۰ به بعد، هر کاربر فقط در صورت مجاز بودن می‌تواند به اطلاعات دسترسی داشته باشد.

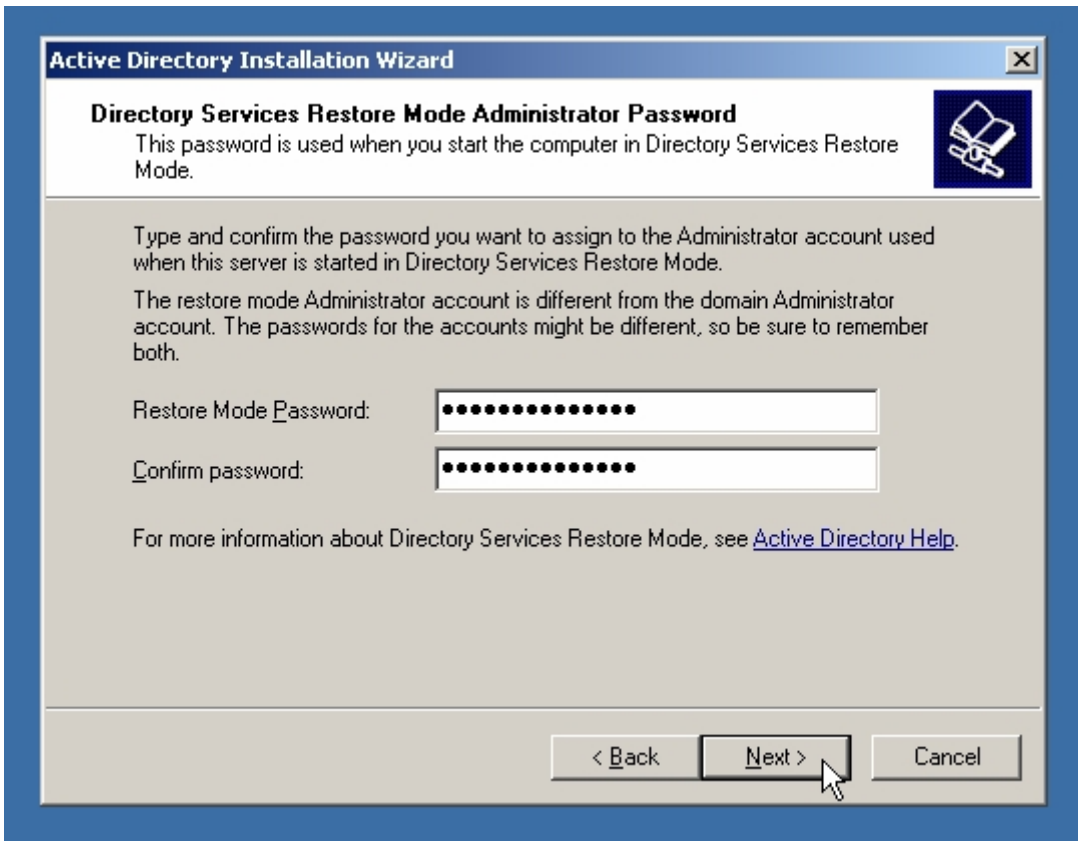
به همین دلیل، در صورتیکه در شبکهٔ ما سرورهای قدیمی وجود داشـته باشـد، ایـن عـدم هـمـاهنگی مـشکل بوجـود خواهـد آورد. بـرای رفـع ایـن مـشکل، سـرویس Active directory به دو صورت می‌تواند فعالیـت کنـد. یـا بـصورتیکه قابـل اسـتفاده بـه همـراه سرورهای قـدیمی‌تـر باشـد ( کـه حفاظـت کمتـری دارد ) یـا در حالتیکـه در شـبکه فقـط سرورهای ۲۰۰۰ و ۲۰۰۳ وجود دارند ( که حفاظت بالاتری دارد ).

در این مثال، ما گزینهٔ دوم را که پیش‌فرض نیز می‌باشد انتخاب می‌کنـیم و دکمـهٔ Next را می‌زنیم.

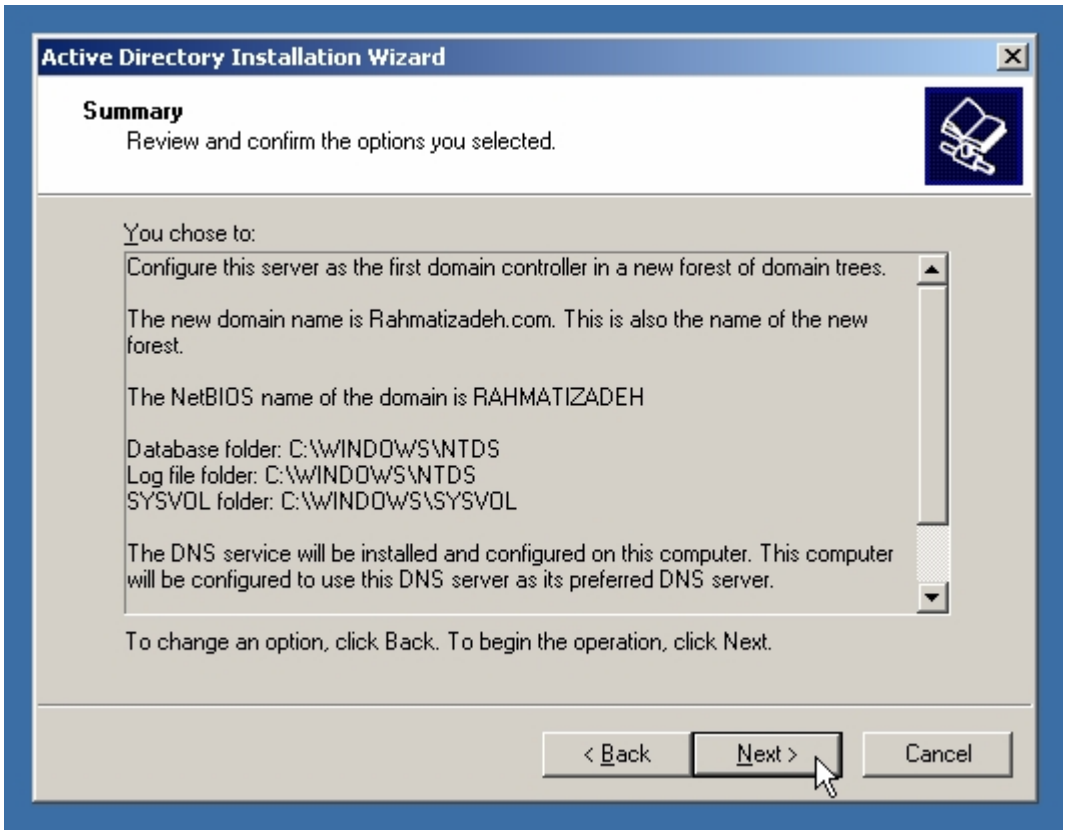


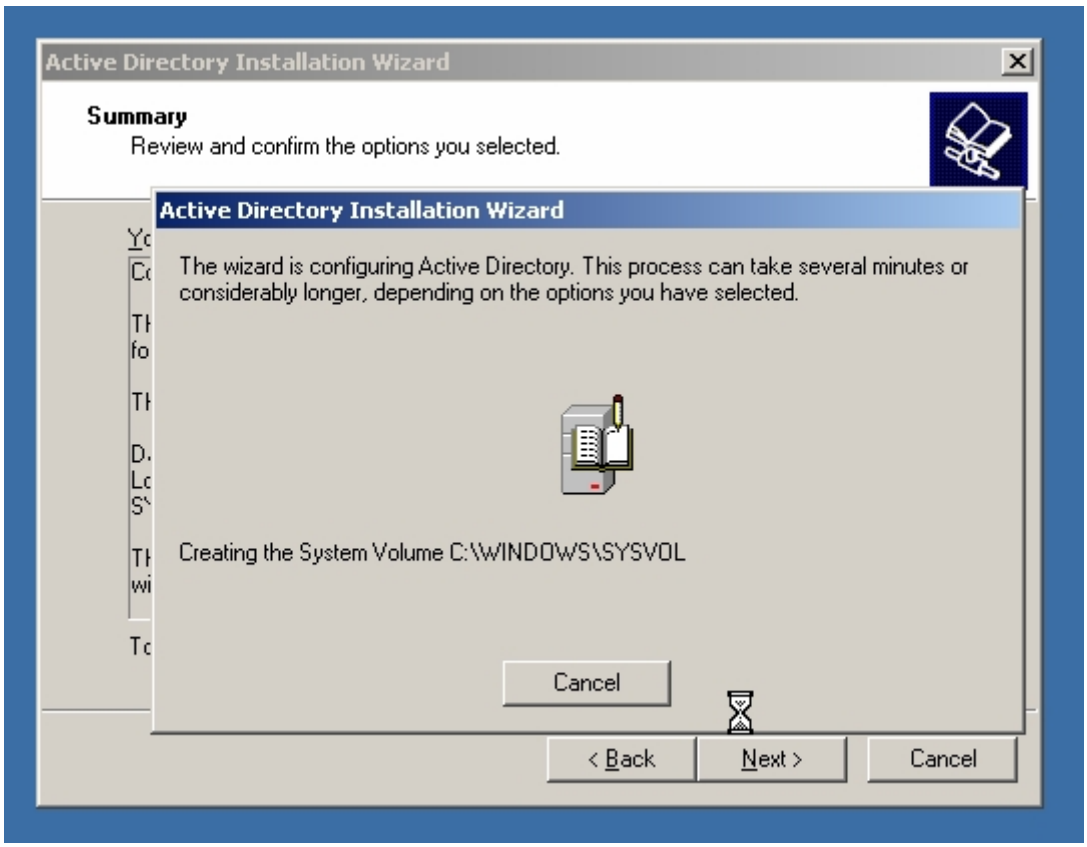

کلیهٔ اطلاعات مربوط به کاربران مختلف در Active directory نگه‌داشته می‌شود. اطلاعات مربوط به Administrator شبکه نیز به همین صورت است. در صورتیکه برای فایل‌های Active directory مشکلی بوجود آید، اطلاعات مربوط به کاربران از بین خواهد رفت. در domain controllerها در هنگام بالا آمدن سیستم‌عامل و با زدن کلید F8، گزینه‌ای تحت عنوان Directory Services Restore Mode وجود دارد، که این امکان را می‌دهد که اطلاعات موجود در Active directory را با یک backup گرفته شده جایگزین کنیم. با توجه به اینکه در این زمان اطلاعات موجود در Active directory، در دسترس نیست، رمز جداگانه‌ای برای این مرحله از کاربر پرسیده می‌شود. در این قسمت ما این رمز را تعیین می‌کنیم.

پس از دوبار وارد کردن رمز، کلید Next را بزنید.

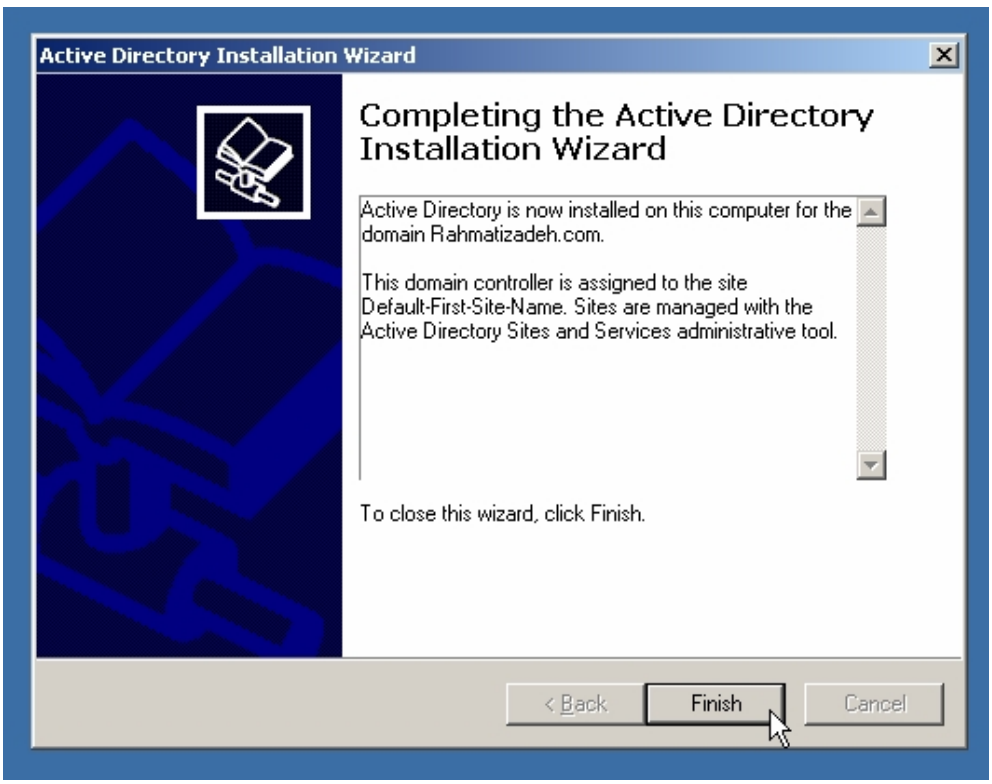


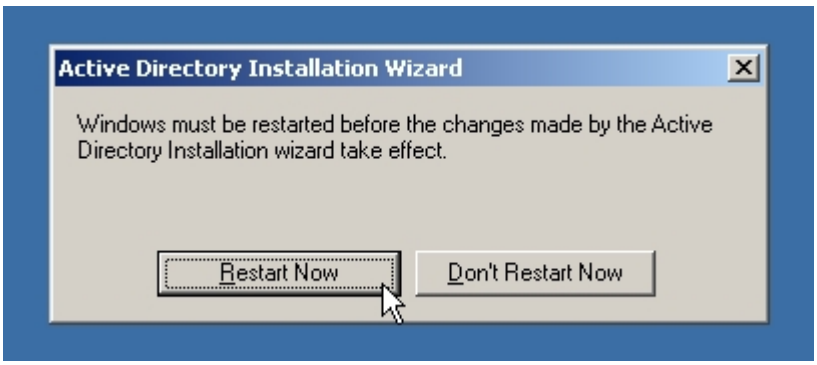

**در انتها، خلاصه‌ای از موارد وارد شده توسط کاربر نشان داده می‌شود. پس از زدن کلید Next، نصب Active directory بر روی سرور آغاز می‌شود.**






پس از پایان، در صورت موفقیت آمیز بودن نصب Active directory پنجرهٔ زیر نمایش داده خواهد شد. پس از زدن دکمهٔ Finish، سرور باید restart شود. پس از restart شدن، سرور ما تبدیل به یک domain controller شده است.






پس از restart شدن دستگاه، اولین تغییری که مشاهده می‌کنید، حذف گزینهٔ Log on to this computer از پنجرهٔ Log on ویندوز است. به domain controllerها نمی‌توان خارج از شبکه لاگین کرد.


- **Objectهای استاندارد موجود در Active Directory**

از objectهای مختلفی که در Active directory وجود دارد، در کلاس شبکهٔ مبتدی، فقط به objectهای خاص می‌پردازیم: Organizational Unitها مانند folderها وظیفهٔ تقسیم‌بندی در Active directory را بعهده دارند. با استفاده از OUها، مدیر شبکه می‌تواند objectهای دیگر را بصورت منطقی از هم جدا کند. معمولا این جداسازی به سه منظور انجام می‌شود: ۱- جداسازی ظاهری جهت تقسیم‌بندی ظاهری و برای راحتتر شدن کار با objectها ۲- جداسازی به منظور اعمال سیاست‌های مختلف بر روی یکدسته از objectهای خاص ۳- مخفی‌سازی تعداد خاصی از objectها در شبکه.

در کلیهٔ حالت‌های ذکر شده، OUها مانند folderها که وظیفهٔ جداسازی فایل‌ها از یکدیگر را دارند، عمل کرده و objectهای مختلف را در Active directory از هم جدا می‌کنند. در ضمن مانند folderها، OUها نیز می‌توانند تو در تو باشند.

Userها، وظیفهٔ نگهداری اطلاعات مربوط به کاربران شبکه را دارند. این اطلاعات شامل نام کاربری، رمز، زمان مجاز جهت استفاده از شبکه، کامپیوترهایی که کاربر مجاز به استفاده از آن‌ها است، عضویت کاربر در گروه‌ها، نام و نام‌خانوادگی، Email، آدرس و غیره است. برای هر کاربر شبکه که می‌خواهد به یکی از کامپیوترهای domain لاگین کند، باید یک object منحصر به فرد در Active directory وجود داشته باشد.

Computerها، محتوی اطلاعات مربوط به کامپیوترهای Domain هستند. مانند کاربران، هر کامپیوتر موجود در Domain نیز باید یک object منحصر به فرد در Active directory داشته باشد.

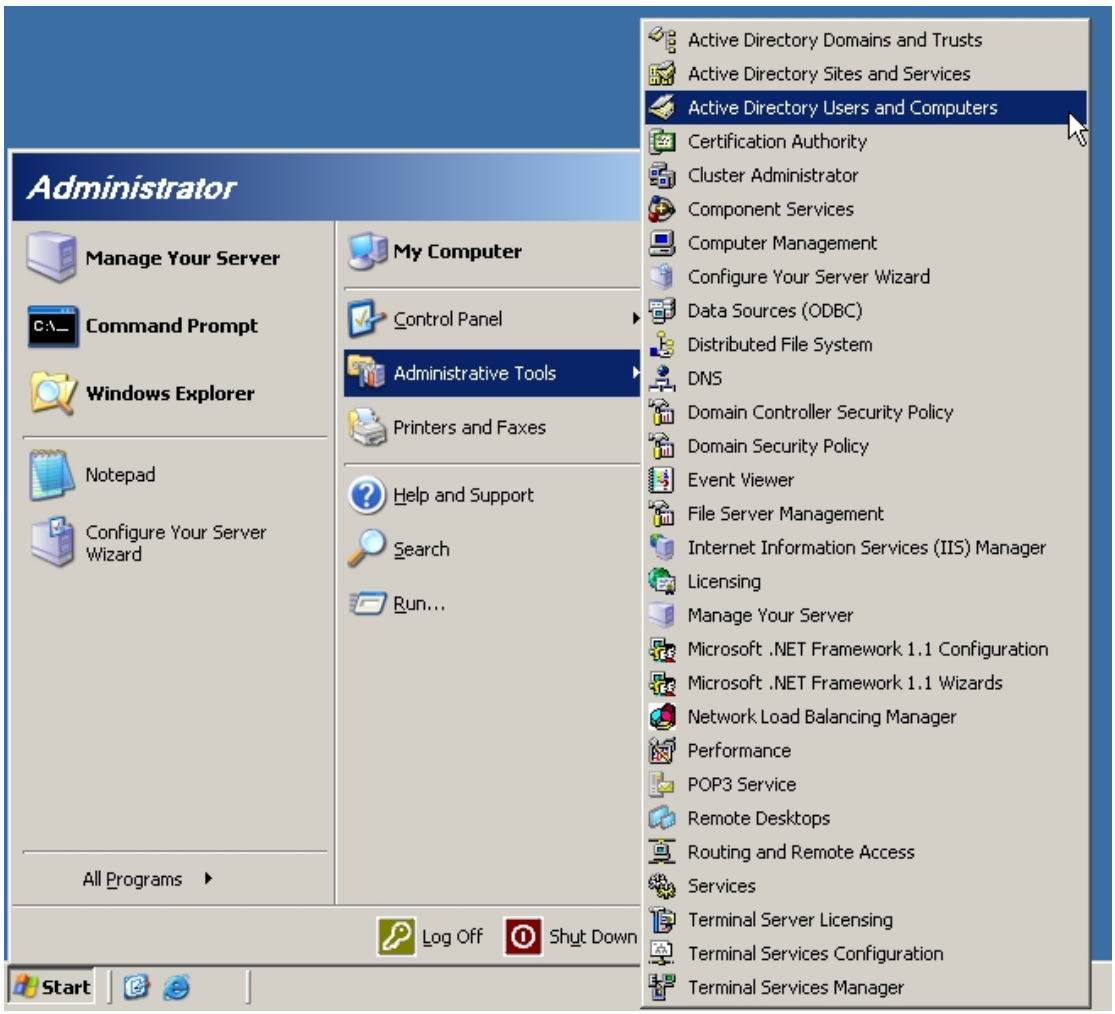
Groupها، جهت دسته‌بندی کاربران و کامپیوترهای موجود در شبکه استفاده می‌شوند. مدیر شبکه می‌تواند برای سهولت کار خود، کاربران و کامپیوترها را در گروه‌های منطقی قرار دهد. برای مثال، مدیر شبکه می‌تواند دو گروه "کاربران عادی" و "کاربران خاص" را تعریف کند. سپس کاربران موجود در Active directory را به عضویت این گروه‌ها درآورد و برای هر گروه شرایط خاصی را تعریف کند. گروه‌ها باعث آسان‌تر شدن کار مدیر شبکه می‌شوند. اگر شبکه‌ای ۲۰۰ کاربر داشته باشد، بجای آنکه برای ۲۰۰ نفر شرایطی تعریف شود، برای یک گروهکه همهٔ این کاربران عضو آن هستند، شرایط تعریف می‌شود.

## o نحوهٔ مدیریت Active Directory

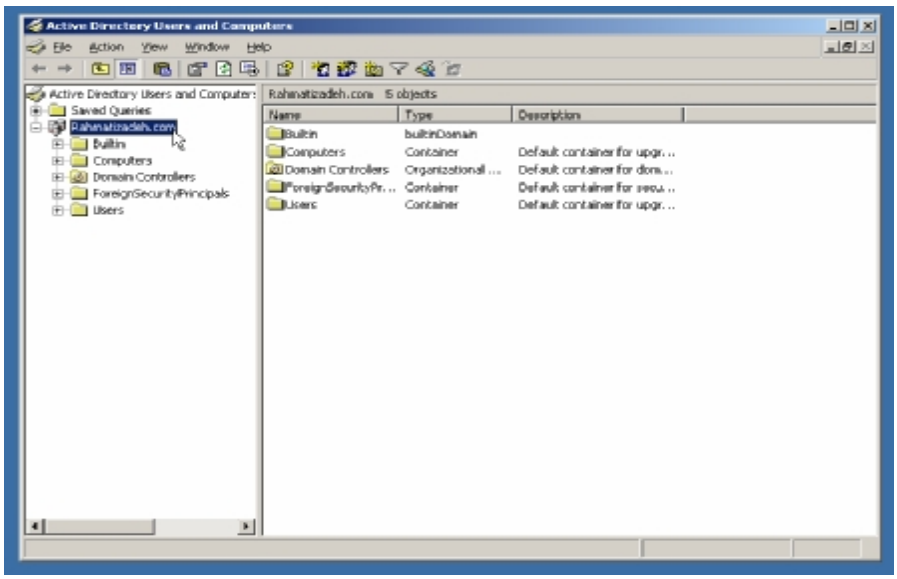
ابزارهای مختلفی جهت مدیریت Active directory در سرورهای ۲۰۰۳ وجود دارد. در این فصل به شرح تعدادی از این ابزارها می‌پردازیم:

### § Active Directory Users and Domains

این ابزار را در منوی Administrative tools می‌توانیم پیدا کنیم.




**با استفاده از این ابزار، می‌توانیم قسمت** domain **موجود در** Active directory **را مدیریت کنیم. پس از انتخاب این گزینه برنامهٔ** mmc **به همراه** snapin، active directory users and computers **اجرا خواهد شد که به دو قسمت چپ و راست تقسیم شده است.**



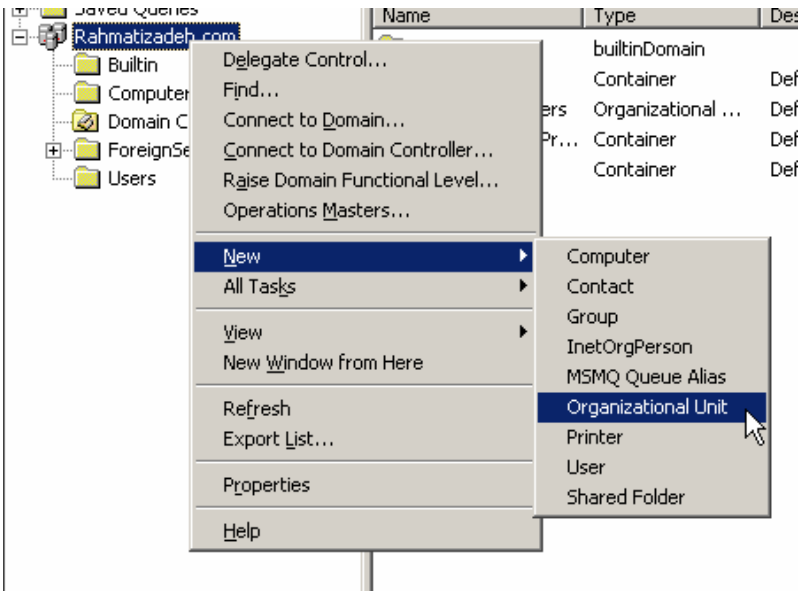
در قسمت سمت راست، بصورت یک نمودار درختی، تقسیم‌بندی‌های موجود در Active directory نمایش داده می‌شود. این تقسیم‌بندی‌ها شامل نام domain و تقسیم‌بندی‌هایی که بطور پیش‌فرض در Active directory وجود دارند – مانند Builtin – و OUهایی که توسط مدیر شبکه ساخته می‌شود است. از علامت‌های زیر به‌ترتیب برای نشان دادن تقسیم‌بندی‌های پیش‌فرض و OUها استفاده می‌شود:



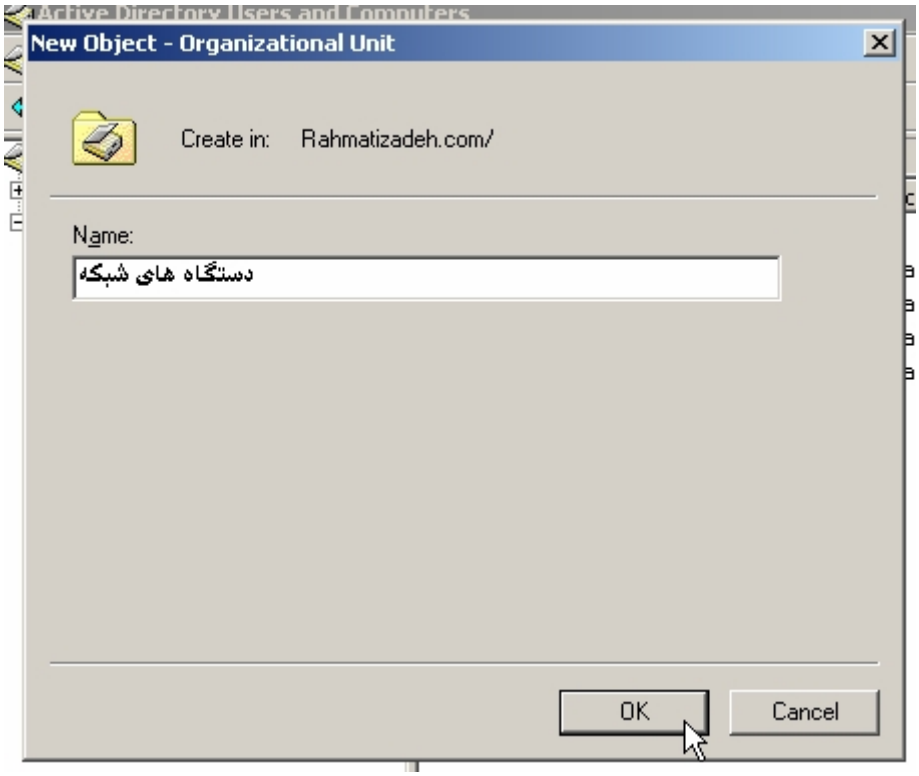
با انتخاب هرکدام از این تقسیم‌بندی‌ها، در قسمت سمت چپ، محتویات آن‌ها نشان داده می‌شود. هر کدام از objectهایی که در قبل گفته شد، دارای علامت خاصی در Active directory users and computers هستند. از علامت  برای نمایش کامپیوترها، از  برای نمایش کاربران و از  برای نشان دادن گروه‌ها استفاده می‌شود.

## § Organizational Units

همانطور که گفته شد از OUها برای تقسیم‌بندی Active directory استفاده می‌شود. جهت ایجاد یک OU جدید، دکمهٔ سمت راست موس را بر روی مکانی که باید OU در آن ایجاد شود می‌زنیم و گزینهٔ New را انتخاب کرده بر روی Organizational Unit کلیک می‌کنیم.



سپس نام OU جدید را وارد می‌کنیم و دکمهٔ OK را می‌زنیم.

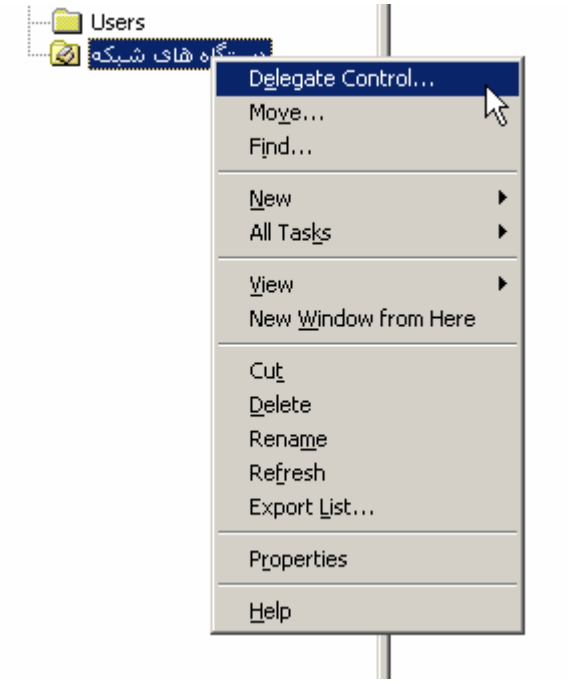



Organization Unit جدید ساخته می‌شود.


به همینصورت می‌توانیم برای عوض کردن اسم، پاک کردن و یا ساختن OU جدید در داخل این OU، عمل کنیم.

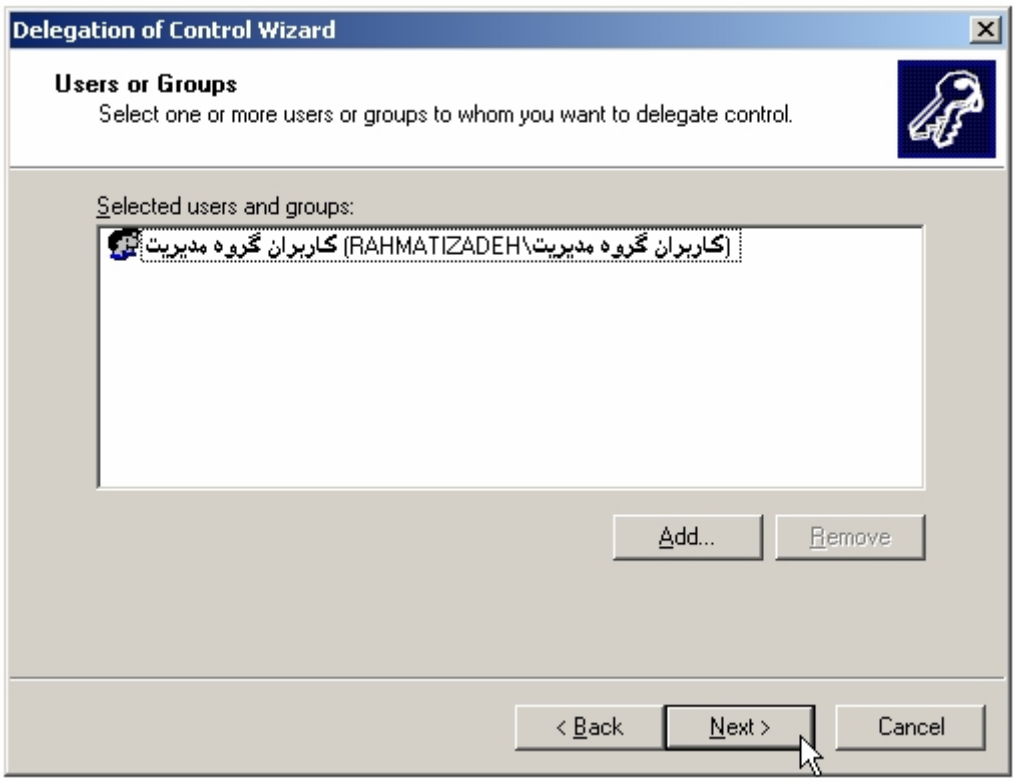
جهت انتقال objectهای مختلف به داخل این OU، می‌توانیم از روش drag&drop استفاده کنیم و یا با کلیک دکمهٔ سمت راست موس، گزینهٔ Move را انتخاب کنیم.

با استفاده از OUها می‌توان مدیریت objectهای داخل آن‌ها را به شخص دیگری محول کرد. این امر به دو روش امکان‌پذیر است. در روش اول، با زدن دکمهٔ سمت راست موس بر روی OU مورد نظر از منوی ظاهر شده، گزینهٔ Delegate control را انتخاب می‌کنیم.

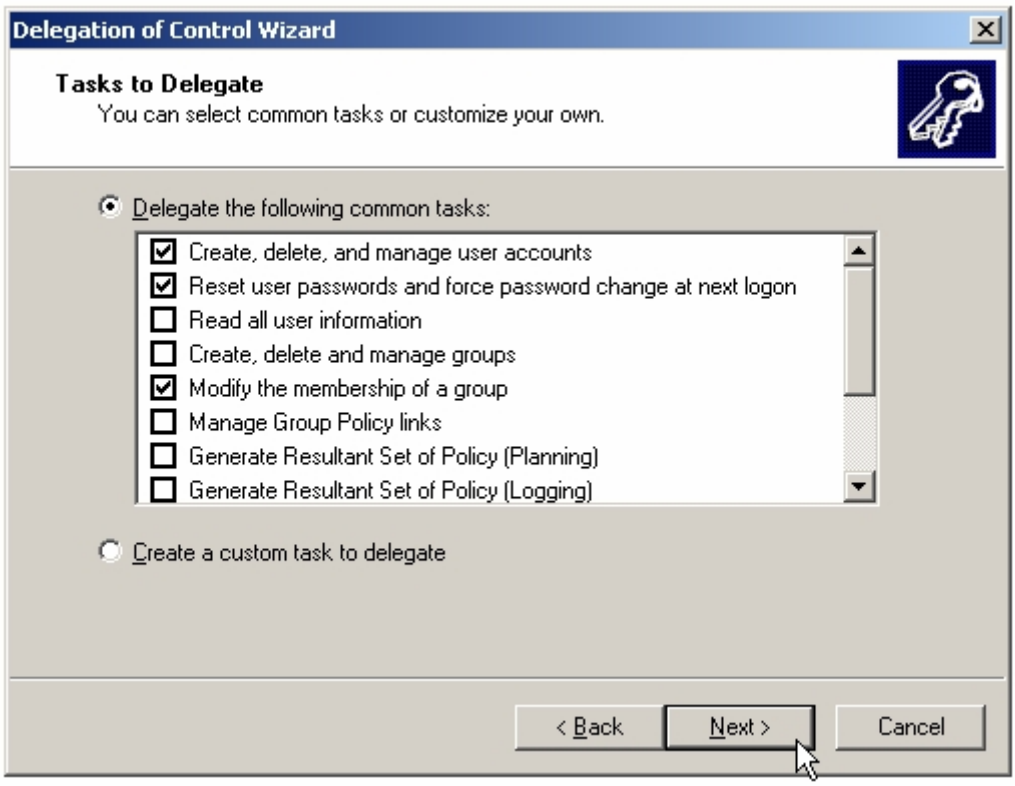



**در اولین صفحهٔ ظاهر شده، دکمهٔ Next را انتخاب می‌کنیم.**


**سپس کاربران یا گروه‌هایی را که می‌خواهیم مدیریت را به آن‌ها محول کنیم را انتخاب می‌کنیم و دکمهٔ Next را می‌زنیم.**

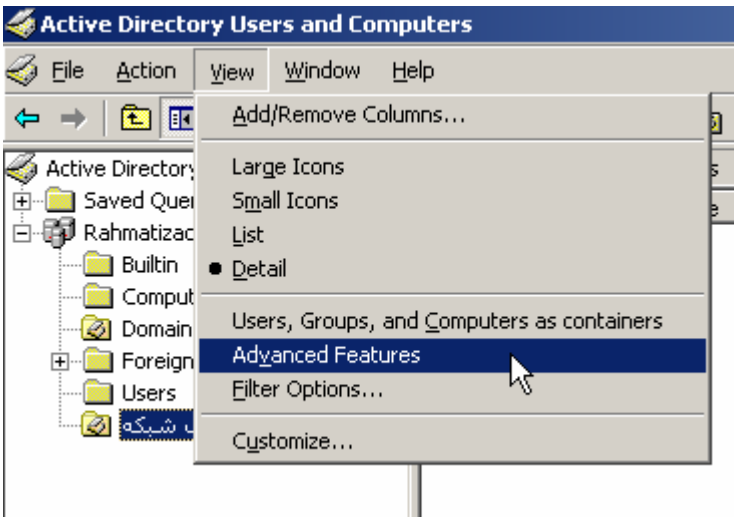



در پنجرهٔ بعدی از بین اعمال متداول و پیش‌فرض مدیریتی، اعمال پیش‌فرض را انتخاب می‌کنیم. در غیراینصورت می‌توان با انتخاب گزینهٔ Create a custom task to delegate، به دلخواه اعمالی را تعریف کنیم.

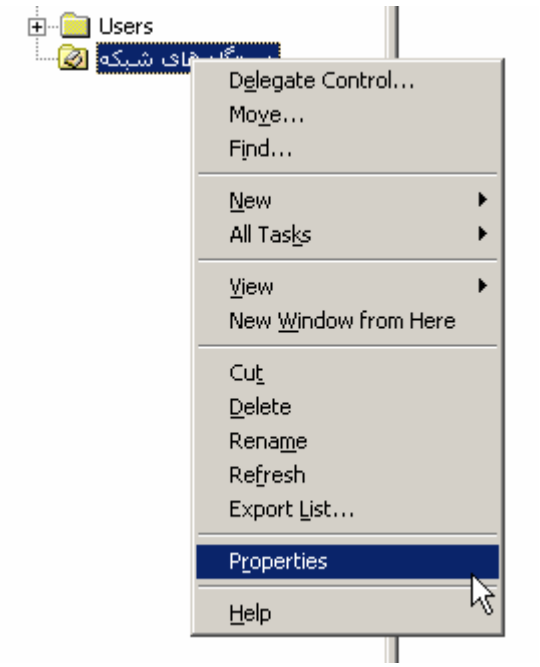


پس از زدن دکمهٔ Finish، اعمال مدیریتی انتخاب شده، فقط برای objectهایی که درون این OU هستند، در کنترل کاربران یا گروه‌هایی که انتخاب کرده‌ایم درمی‌آیند.

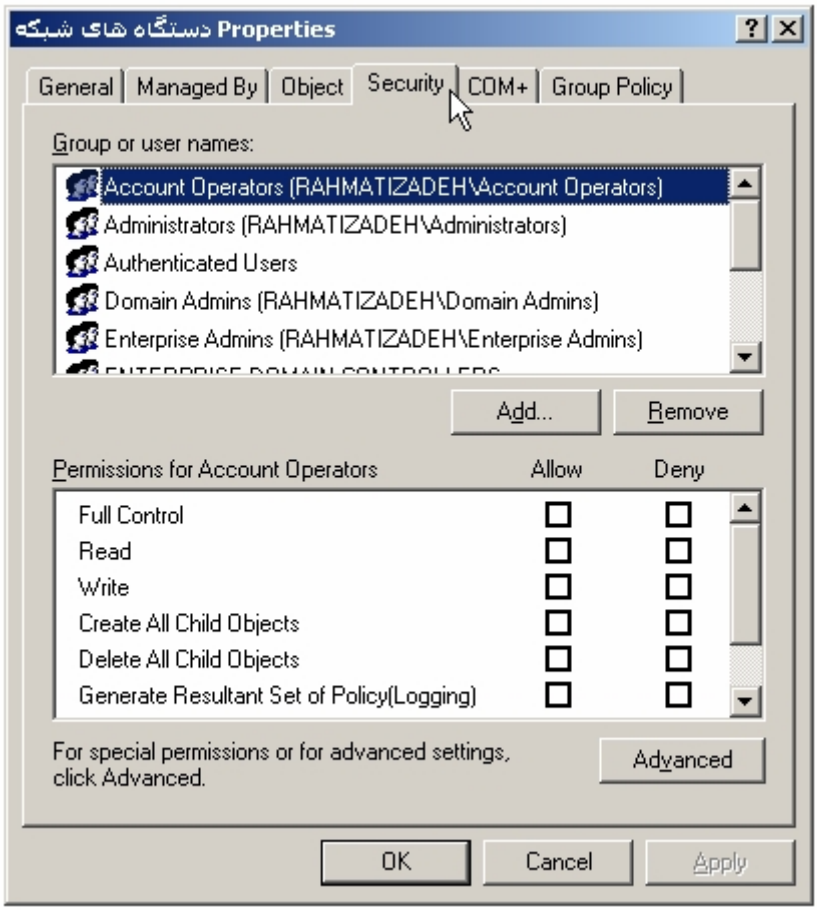

در روش دوم، ابتدا منوی view را باز کرده، گزینهٔ advanced features را انتخاب می‌کنیم.




سپس بر روی OU مورد نظر دکمهٔ سمت راست موس را می‌زنیم و از منوی ظاهر شده، گزینهٔ Properties را انتخاب می‌کنیم.




در پنجرهٔ ظاهر شده، سربرگ Security را انتخاب می‌کنیم. در لیست بالایی، نام کاربران یا گروه‌هایی را که می‌خواهیم اضافه می‌کنیم و در لیست پایین، دسترسی‌های لازم را به هرکدام می‌دهیم.



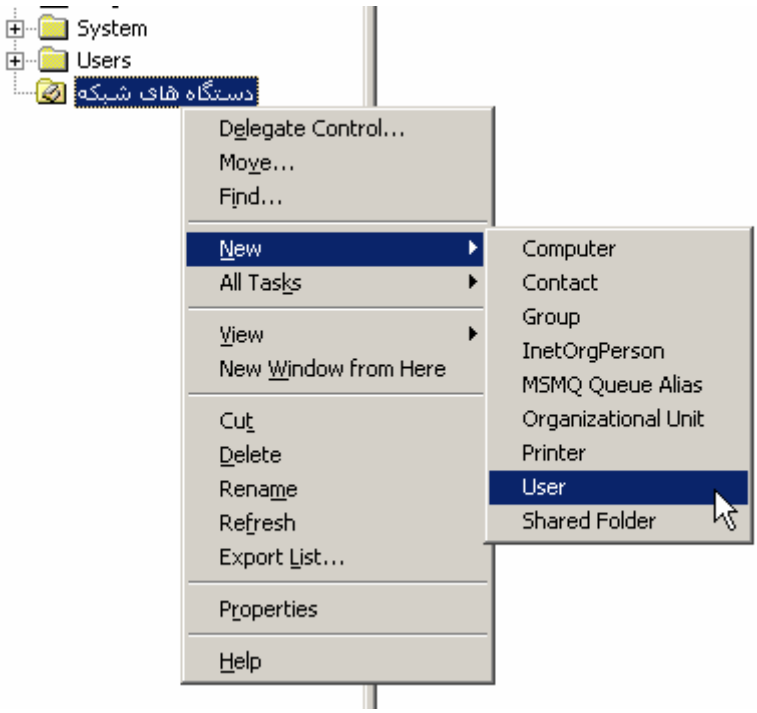
یکی دیگر از دلایل استفاده از OUها اعمال سیاست‌های خاص بر روی گروهی از Objectها می‌باشد. این Objectها را درون یک OU قرار داده و سیاست‌های خاص این OU را تعریف می‌کنیم. توضیحات کامل در مورد سیاست‌های شبکه، در قسمت Group policy داده می‌شود.

یکی دیگر از دلایل استفاده از OUها، مخفی کردن بعضی از Objectها می‌باشد. به ترتیبی که گفته شد، اگر در سربرگ security، دسترسی‌های گروهی را حذف کنیم یا از نوع deny تعریف کنیم، این گروه نمی‌تواند به این OU و Objectهای درون آن دسترسی داشته باشد.

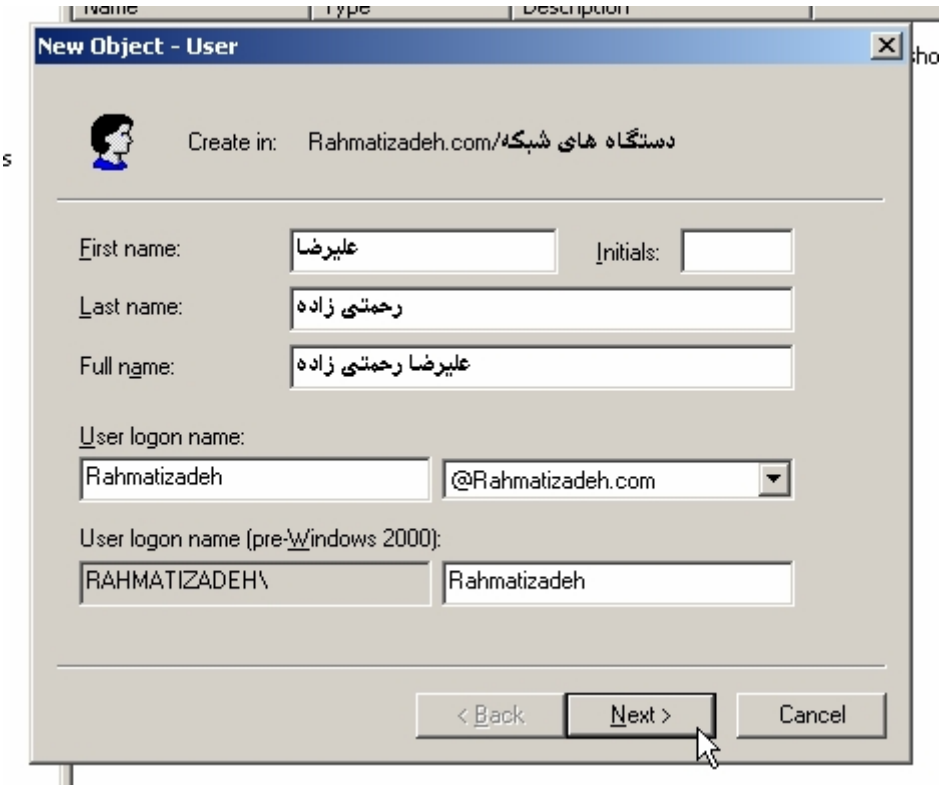
## § Users

هر کاربر توسط یک object در Active directory نمایش داده می‌شود. این object مشخصات مختلفی را در مورد هر کاربر نگهداری می‌کند. جهت اضافه کردن کاربری با نام علیرضا رحمتی‌زاده به Active directory، به روش زیر عمل می‌کنیم:

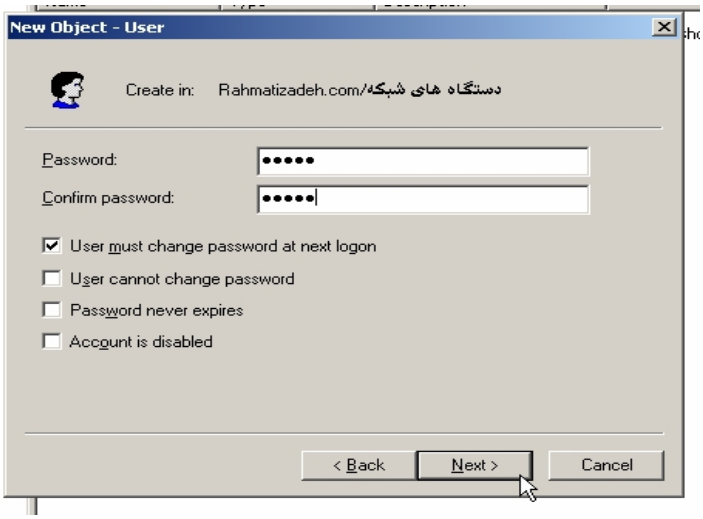
ابتدا OU مورد نظر را انتخاب کرده و بر روی آن دکمهٔ سمت راست موس را می‌زنیم. سپس از منوی باز شده گزینهٔ New و سپس User را انتخاب می‌کنیم.




سپس در پنجرهٔ ظاهر شده گزینه‌های مختلف را تکمیل می‌کنیم و دکمهٔ Next را می‌زنیم. توجه کنید که قسمتهای user logon name، نامی است که کاربر هنگام login کردن به شبکه در ویندوز استفاده می‌کند.

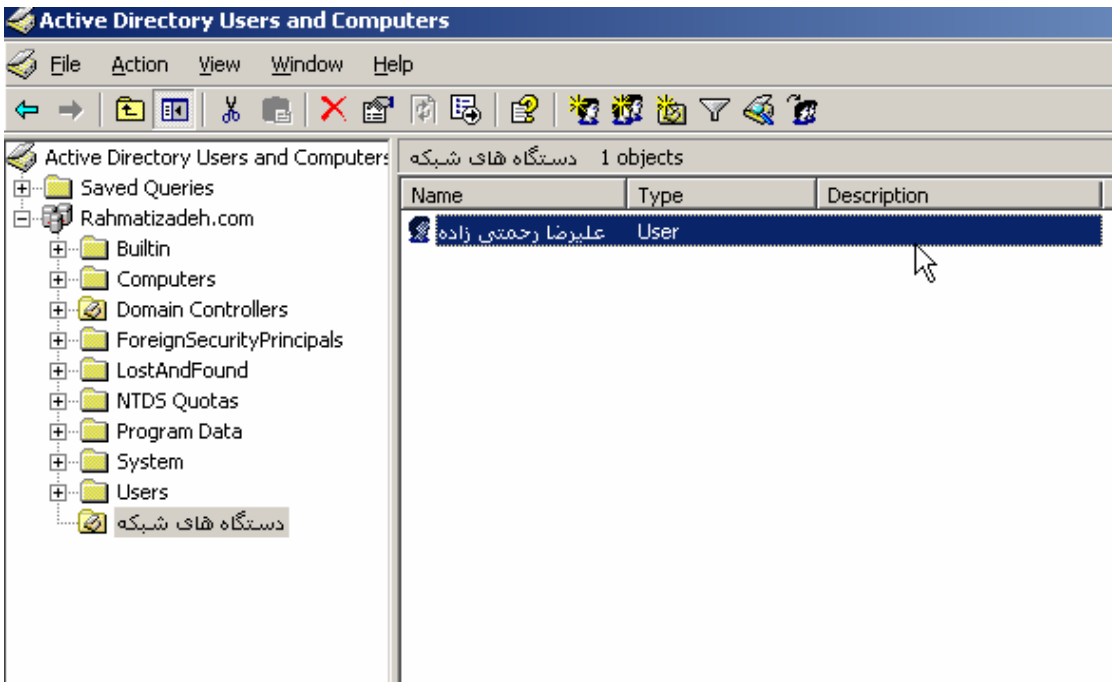



در پنجرهٔ بعدی، رمز کاربر را دوبار وارد می‌کنیم. عبارت User must change password at next logon، به معنی این است که کاربر باید در اولین Login، رمز خود را عوض کند. ویندوز تا هنگامی‌که کاربر رمز خود را عوض نکرده است، به وی اجازه کار نمی‌دهد. در صورتیکه بخواهیم امکان عوض کردن رمز را از کاربر بگیریم، گزینهٔ User cannot change password و اگر بخواهیم اعتبار رمز کاربر تمام نشود(این گزینه در قسمت‌های بعدی به تفصیل توضیح داده خواهد شد)، گزینهٔ Password never expires و اگر بخواهیم کاربر غیر فعال باشد ( نتواند Login کند) گزینهٔ account is disabled را انتخاب می‌کنیم. برای اتمام کار گزینهٔ Next را می‌زنیم.

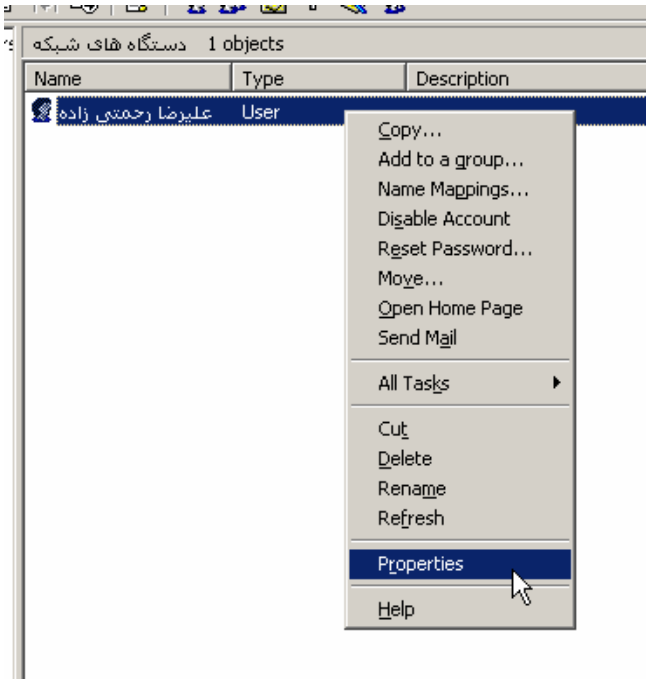


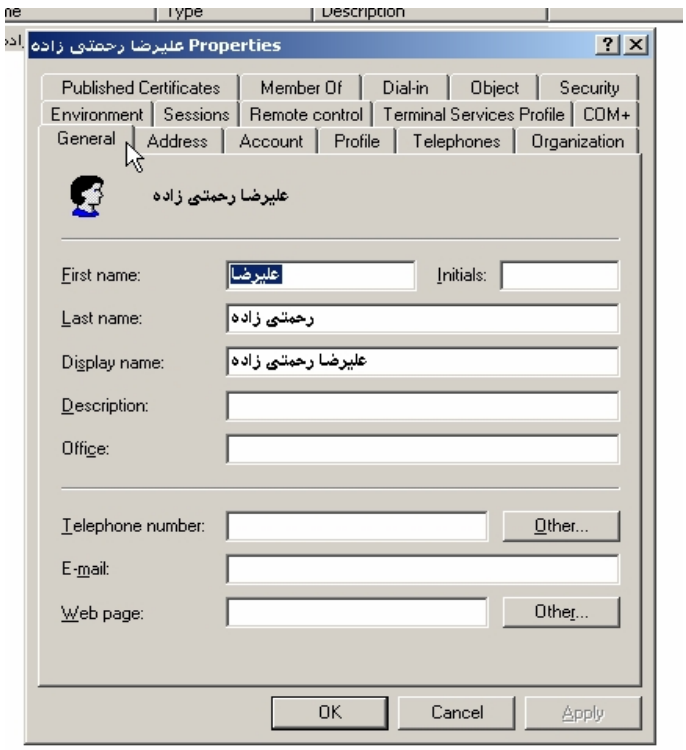
در آخرین پنجره خلاصه‌ای از آنچه انتخاب شده نمایش داده می‌شود. با زدن دکمهٔ Finish کاربر جدید ساخته می‌شود.


اکنون کاربر علیرضا رحمتی‌زاده، می‌تواند در کامپیوترهایی که در شبکه وجود دارند، با نام کاربری Rahmatizadeh و رمز مخصوص خود login کند. Object مخصوص این کاربر، در OU، دستگاه‌های شبکه ساخته شده است.



اطلاعاتی که Active directory در مورد هر کاربر نگه می‌دارد، محدود بـه عنـاوین ذکر شده نیست. اکنون اگر بر روی کاربر مورد نظـر دکمـهٔ سـمت راسـت مـوس را بزنیم و گزینهٔ properties را انتخاب کنیم، اطلاعات کاملتری را در مورد هر کاربر می‌توانیم وارد کنیم (توجه داشته باشید که در تمرین‌های قبلـی گزینـهٔ advanced features را از منوی view فعال کرده‌ایم)



**قسمت‌های مختلف این پنجره و کـاربرد آن‌هـا در قـسمت‌هـای بعـدی توضـح داده خواهد شد.**