

فهرست

| | | |
|---------|--|---|
| ۳..... | مقدمه | |
| ۵..... | پیش‌نیازها | |
| ۶..... | نام کامپیوتر (COMPUTER NAME) | • |
| ۹..... | اینترنت پروتوکل یا IP | • |
| ۱۴..... | مفهوم SUBNET MASK | • |
| ۱۶..... | مفهوم GATEWAY | • |
| ۱۷..... | تنظیمات DNS | • |
| ۱۸..... | شبکه‌های مبتنی بر DOMAIN | |
| ۲۰..... | سرویس ACTIVE DIRECTORY | • |
| ۲۰..... | کاربرد | ○ |
| ۲۰..... | پیش‌نیازهای راه‌اندازی سرویس ACTIVE DIRECTORY | ○ |
| ۲۱..... | نحوه راه‌اندازی سرویس ACTIVE DIRECTORY | ○ |
| ۲۷..... | نصب سرویس ACTIVE DIRECTORY | ○ |
| ۳۷..... | OBJECT های استاندارد موجود در ACTIVE DIRECTORY | ○ |
| ۳۸..... | نحوه مدیریت ACTIVE DIRECTORY | ○ |
| ۳۸..... | Active Directory Users and Domains | § |
| ۴۰..... | Organizational Units | § |
| ۴۶..... | Users | § |

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 دانشجویان را تشویق به خودآموزی می‌کند، پیشنهاد می‌شود که این جزوه، تنها بعنوان منبعی جهت یادگیری اولیه استفاده شود و دانشجوی خود نسبت به فراگیری کامل این مباحث اقدام نماید.

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

این کلاس، تنها به مباحث نرم‌افزاری طراحی و راه‌اندازی شبکه ویندوز NT می‌پردازد و دانشجویان باید خود نسبت به فراگیری نکات سخت‌افزاری اقدام نمایند.

این جزوه توسط نرم‌افزار Microsoft word تهیه شده و کلیه 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 جزوه جداگانه‌ای جهت توضیح نرم‌افزار MVPC و PDF Factory تهیه شود.

پیش نیازها

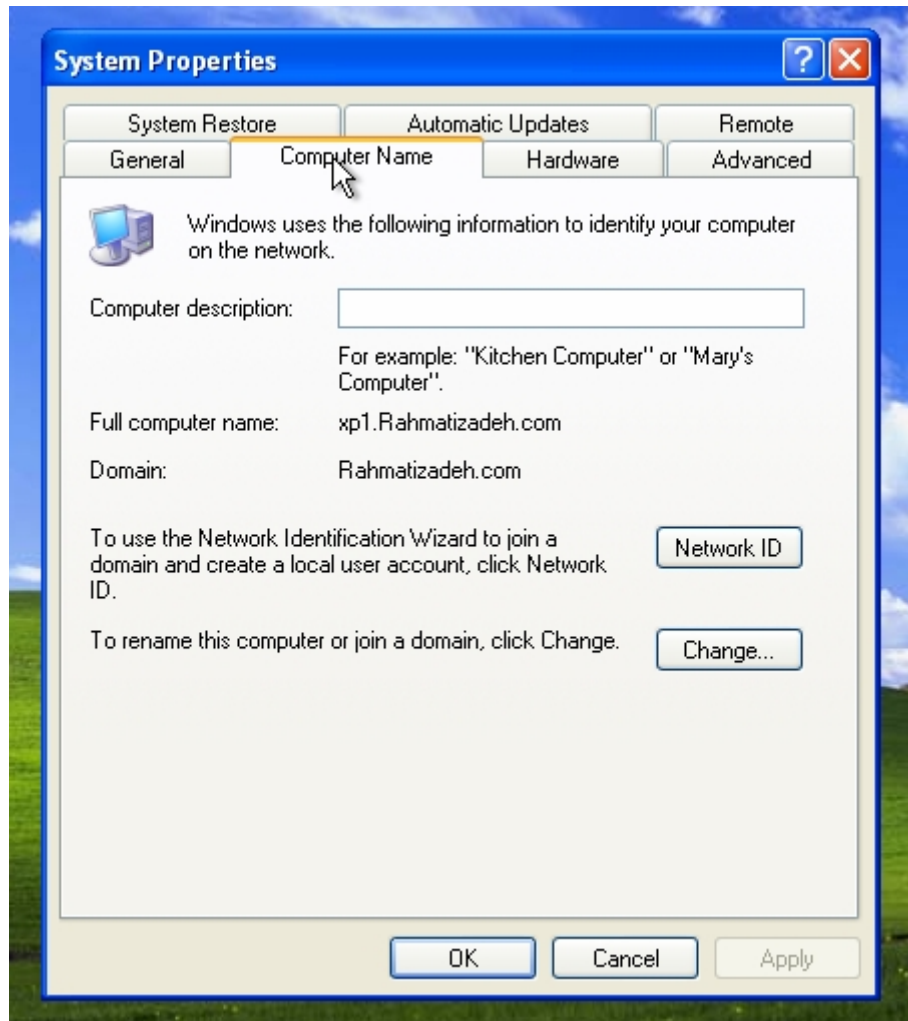
در ابتدای این جزوه، لازم است که مباحثی که بصورت پیش‌نیاز برای شروع راه‌اندازی شبکه مورد نیاز است، بطور اختصار توضیح داده شود:

• نام کامپیوتر (Computer Name)

هر کامپیوتر در شبکه، دارای نام منحصر بفرد می‌باشد. از این نام می‌توان جهت ارتباط با کامپیوتر، در داخل شبکه استفاده کرد. جهت مشاهده یا تغییر نام کامپیوتر، پس از لاگین کردن با کاربر Administrator، به روش زیر عمل کنید :



بر روی دکمه Start کلیک کرده و بر روی علامت My Computer، دکمه سمت راست موس را بزنید. سپس گزینه Properties را انتخاب کنید.



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

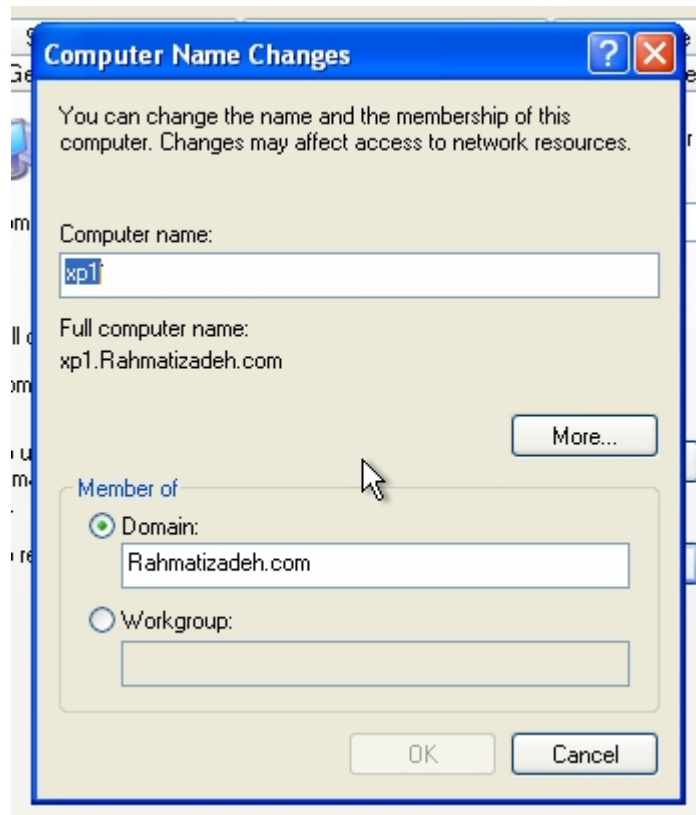
Full computer name: xp1.Rahmatizadeh.com

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 دکمه Change کلیک کنید:

To rename this computer or join a domain, click Change.

Change...



در قسمت Computer name نام کامپیوتر و در قسمت Domain نام Domain ای را که کامپیوتر عضو آن می باشد، 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 سیاست های 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 اجازه 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 می تواند از ۱۵ حرف بیشتر باشد.
- پس از تعویض نام کامپیوتر، به شرطی که کامپیوتر هم نامی در شبکه وجود نداشته باشد، کامپیوتر باید Restart شده تا نام جدید مورد استفاده قرار گیرد.

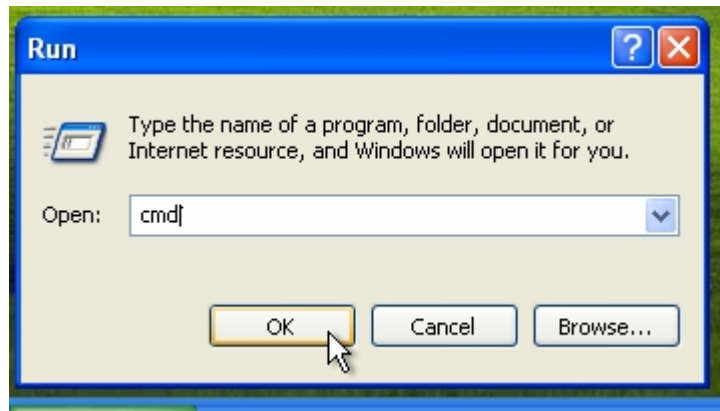
• اینترنت پروتوکل یا IP

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:

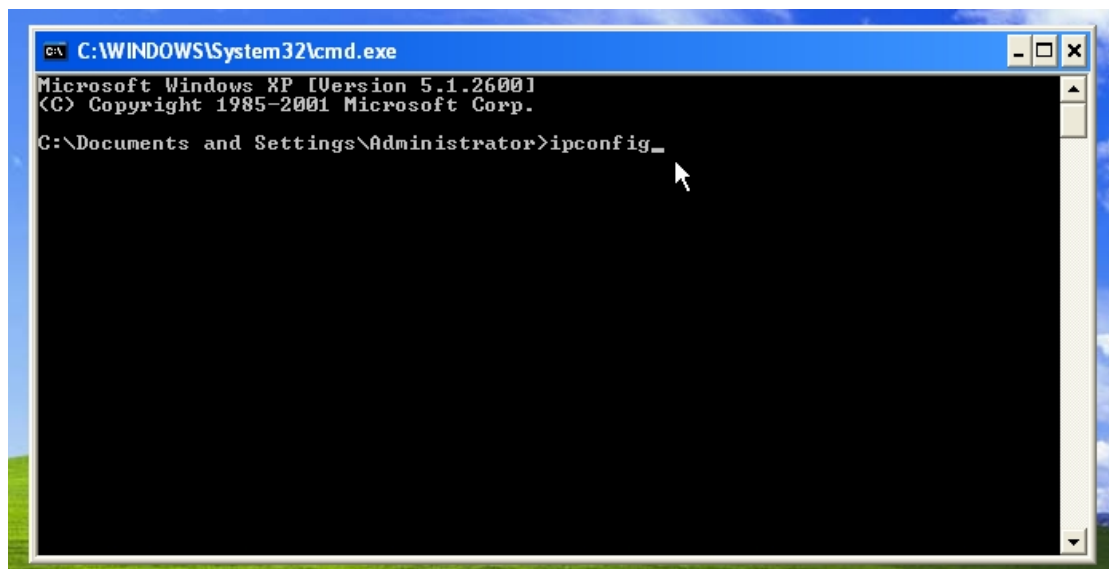
192 . 168 . 0 . 5

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

در روش اول از منوی Start گزینه Run را انتخاب کنید و کلمه cmd را تایپ کنید و کلید OK را فشار دهید.



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



```

C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

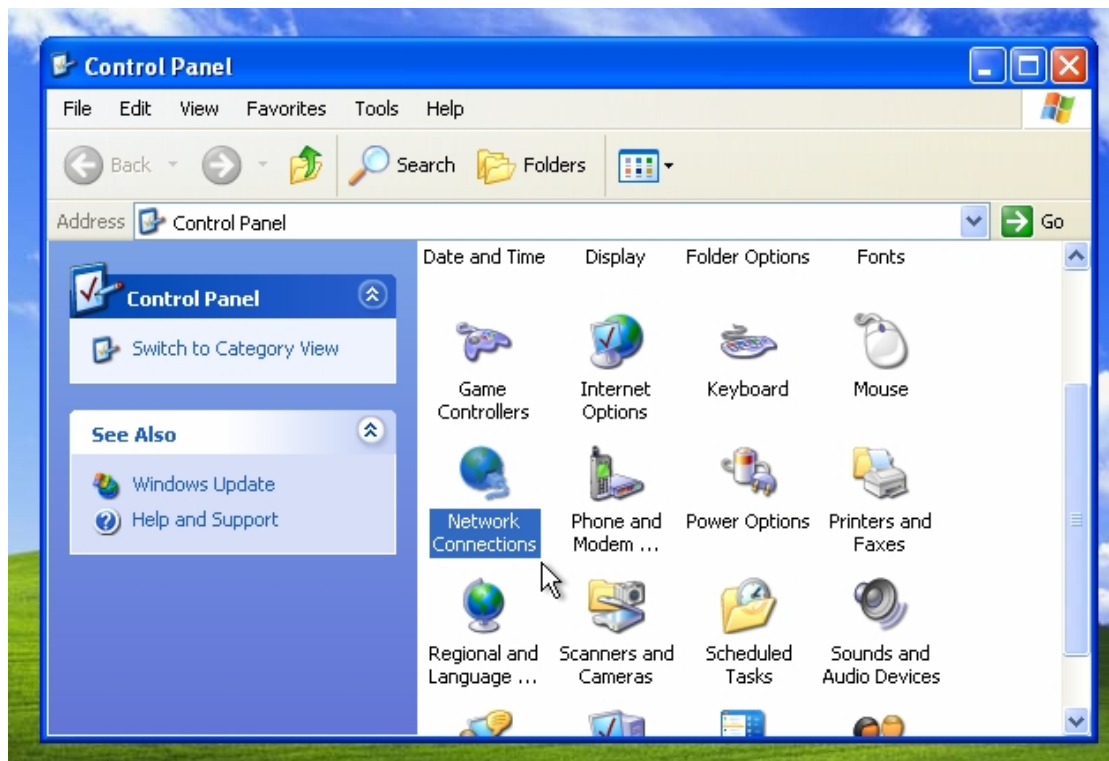
    Connection-specific DNS Suffix  . :
    IP Address . . . . . : 192.168.0.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

C:\Documents and Settings\Administrator>_

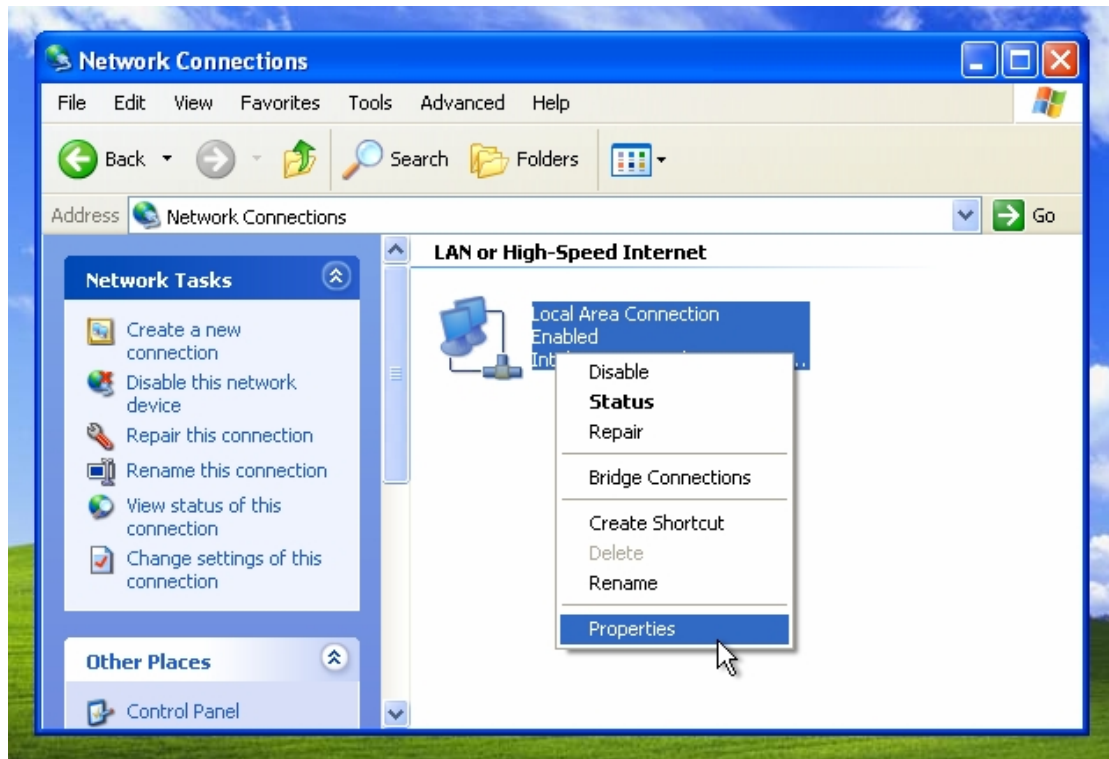
```

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

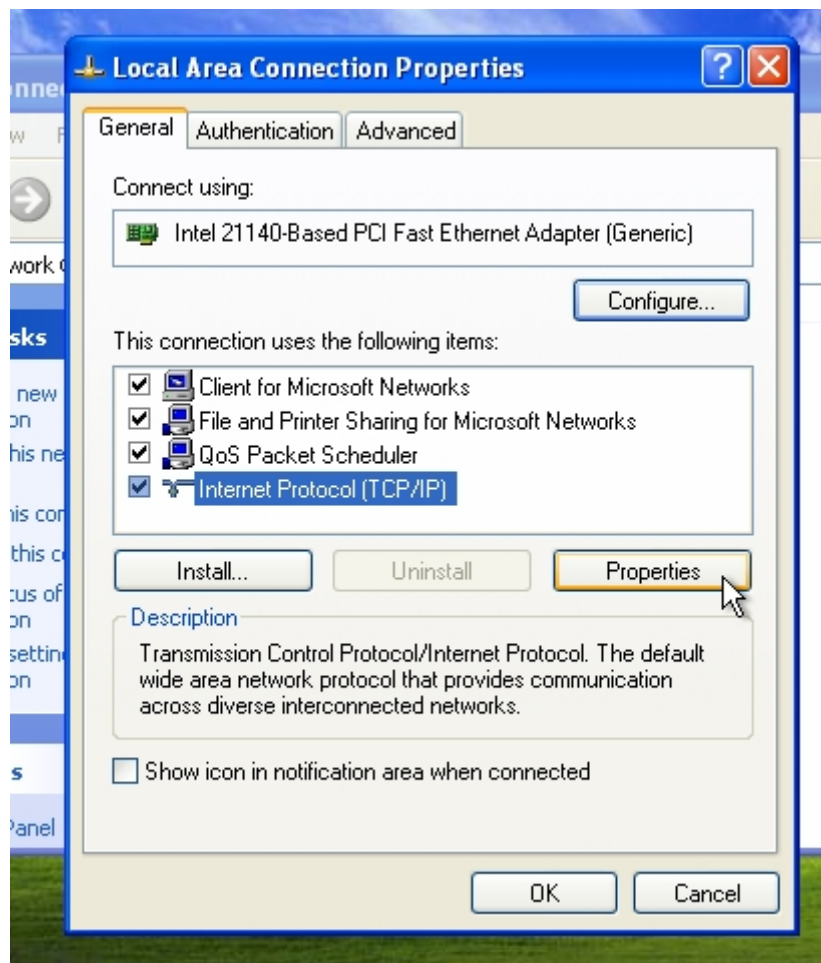
در روش دوم، از منوی Start وارد Control panel شوید و علامت Network connections را انتخاب کنید.



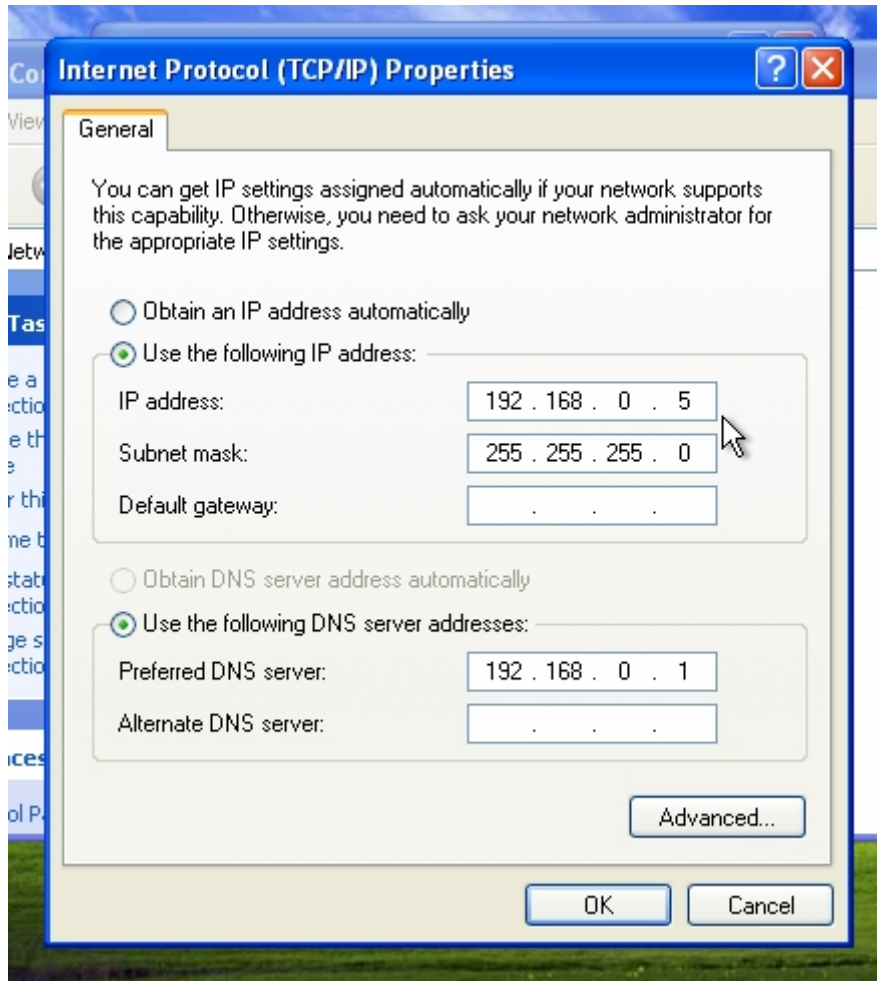
سپس در پنجره ظاهر شده، بر روی علامت کارت شبکه، دکمه سمت راست موس را بزنید و گزینه Properties را انتخاب کنید.



در پنجره ظاهر شده، از لیست موجود، گزینه (TCP/IP) Internet Protocol را انتخاب کنید و دکمه Properties را کلیک کنید.

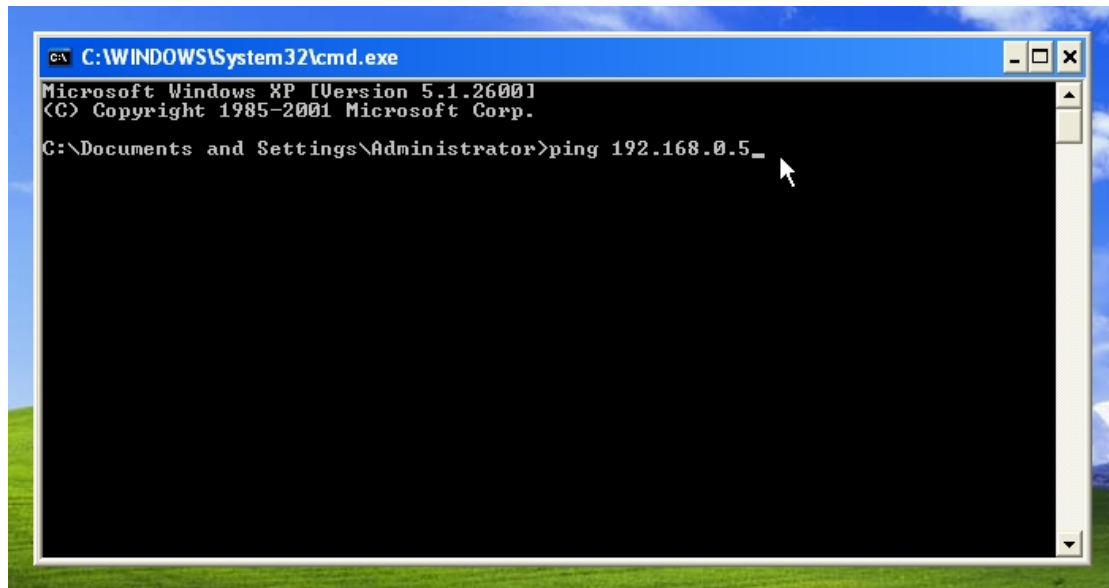


در پنجره بعدی، اعداد ذکر شده در روبروی IP Address، نشان دهنده IP کامپیوتر می‌باشند.

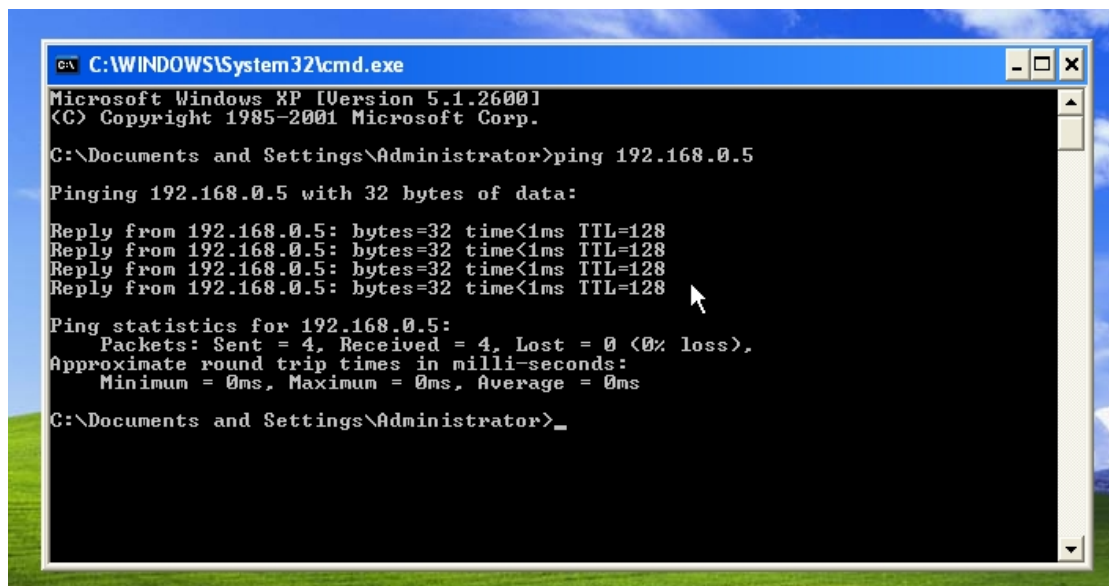


در این پنجره با وارد کردن اعداد جدید، می‌توانید IP کامپیوتر خود را تغییر دهید. فقط باید توجه داشته باشید که این IP، نباید برای کامپیوتر دیگری استفاده شده باشد. برای اعمال تغییرات IP نیازی به Restart کردن کامپیوتر نیست.

به عنوان یک تمرین ساده، می‌توانید بر روی یک کامپیوتر دیگر در شبکه، گزینه Run را از منوی Start انتخاب کنید. سپس عبارت cmd را وارد کنید و کلید OK را انتخاب کنید. در پنجره ظاهر شده، عبارت "Ping xxxx" را وارد کنید (بجای xxxx، IP کامپیوتر خود را تایپ کنید). سپس کلید Enter را بزنید.



```
C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>ping 192.168.0.5_
```



```
C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>ping 192.168.0.5
Pinging 192.168.0.5 with 32 bytes of data:
Reply from 192.168.0.5: bytes=32 time<1ms TTL=128
Reply from 192.168.0.5: bytes=32 time<1ms TTL=128
Reply from 192.168.0.5: bytes=32 time<1ms TTL=128
Reply from 192.168.0.5: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.0.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Documents and Settings\Administrator>
```

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 بیتی تشکیل شده است. پس اعداد تشکیل دهنده Subnet mask نیز هر کدام بین صفر تا ۲۵۵ می‌باشند. هدف از subnet mask، تعیین دامنه شبکه و یا تقسیم شبکه به چند شبکه 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 :

| | |
|--------------|---------------------|
| IP address: | 192 . 168 . 0 . 5 |
| Subnet mask: | 255 . 255 . 255 . 0 |

اعداد موجود در Subnet mask، یک به یک با اعداد موجود در IP، متناظر می‌باشند. عدد ۲۵۵ موجود در Subnet mask، نشاندهنده ثابت بودن عدد متناظر آن در IP، در کل شبکه است. به عبارت دیگر، IP کلیه 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 :

$$\text{Host ID} = 5 = 00000101 \text{ (binary)}$$

$$0 = 00000000 \text{ (binary)}$$

$$00000101 + 00000000 = 00000101$$

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

| | |
|--------------|---------------------|
| IP address: | 192 . 168 . 0 . 255 |
| Subnet mask: | 255 . 255 . 255 . 0 |

در این مثال :

$$\text{Host ID} = 255 = 11111111 \text{ (binary)}$$

$$0 = 00000000 \text{ (binary)}$$

$$11111111 + 00000000 = 11111111$$

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

| | |
|--------------|---------------------|
| IP address: | 192 . 168 . 0 . 0 |
| Subnet mask: | 255 . 255 . 255 . 0 |

در این مثال :

Host ID = 0 = 00000000 (binary)

0 = 00000000 (binary)

00000000 + 00000000 = 00000000

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

| | |
|--------------|-----------------------|
| IP address: | 192 . 168 . 0 . 3 |
| Subnet mask: | 255 . 255 . 255 . 252 |

در این مثال :

Host ID = 3 = 00000011 (binary)

252 = 11111100 (binary)

00000011 + 11111100 = 11111111

این مثال نیز بدلیل ۱ بودن کلیه 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 اهای موجود در باینری آن‌ها می‌باشد. اولاً 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. دوماً کلیه ۱‌های 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 شبکه خود وجود دارند تشخیص داده و با آن‌ها مستقیماً ارتباط برقرار می‌کند.

• مفهوم Gateway

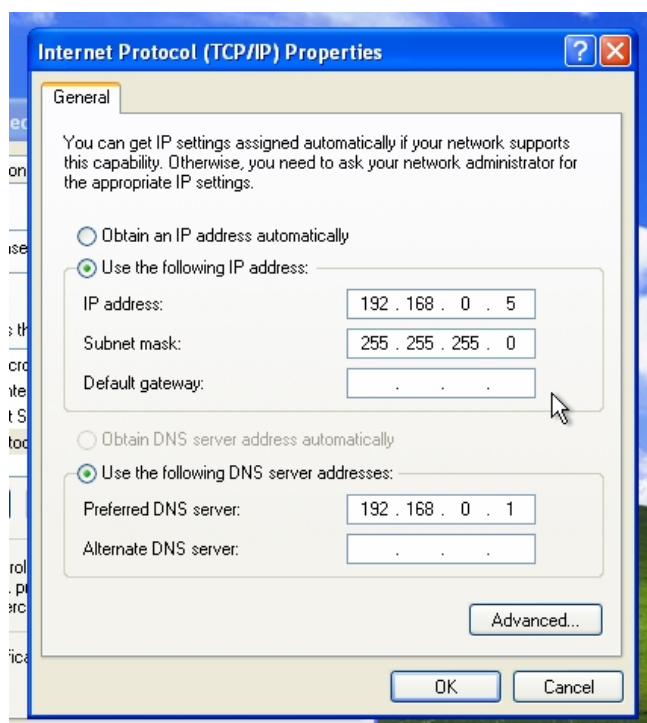
در بخش مربوط به IP، توضیح داده شد که کامپیوتر از ترکیب IP و Subnet mask خود، می‌تواند تشخیص دهد که چه IP‌هایی در شبکه خود وجود دارد. به عنوان مثال، هنگامیکه کامپیوتری با مشخصات زیر بخواهد با کامپیوتری با IP، 192.168.0.18 ارتباط برقرار کند،

| | |
|--------------|---------------------|
| IP address: | 192 . 168 . 0 . 5 |
| Subnet mask: | 255 . 255 . 255 . 0 |

می‌تواند تشخیص دهد که این کامپیوتر در شبکه خود وجود دارد. پس مستقیماً 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 شبکه تعریف شده برای این کامپیوتر وجود ندارد. پس این کامپیوتر نمی‌تواند مستقیماً با آن ارتباط برقرار کند. کامپیوتر مجبور است برای برقراری ارتباط از یک واسطه بنام Gateway استفاده کند. واقعاً، کامپیوتر این درخواست را برای gateway فرستاده، و gateway بجای کامپیوتر این ارتباط را برقرار می‌کند.

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



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

IP ای 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. مخصوصاً در شبکه‌هایی که تعداد کامپیوترهای آن‌ها زیاد است، بخاطر سپردن IP‌های کامپیوترهای مختلف، کار ساده‌ای نیست. معمولاً به خاطر سپردن اسامی، راحتتر از IP است. به همین دلیل در شبکه از سرویسی بنام DNS استفاده می‌شود که این سرویس، وظیفه تبدیل اسامی به IP را در شبکه دارد. این سرویس، معمولاً بر روی یک کامپیوتر مجزا در شبکه وجود دارد. هنگامیکه کامپیوتر ما بخواهد، مثلاً 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 پنجره 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 کلیه کامپیوترها عضوی از یک Domain خاص می‌باشند. در این نوع شبکه‌ها، کنترل کلیه 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 workgroup، در شبکه‌های Domain، کلیه 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 وظیفه 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 اشیاء 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، کلیه کاربران و کامپیوترهای موجود در شبکه، از یک مکان قابل مدیریت هستند.

○ پیش‌نیازهای راه‌اندازی سرویس *Active Directory*

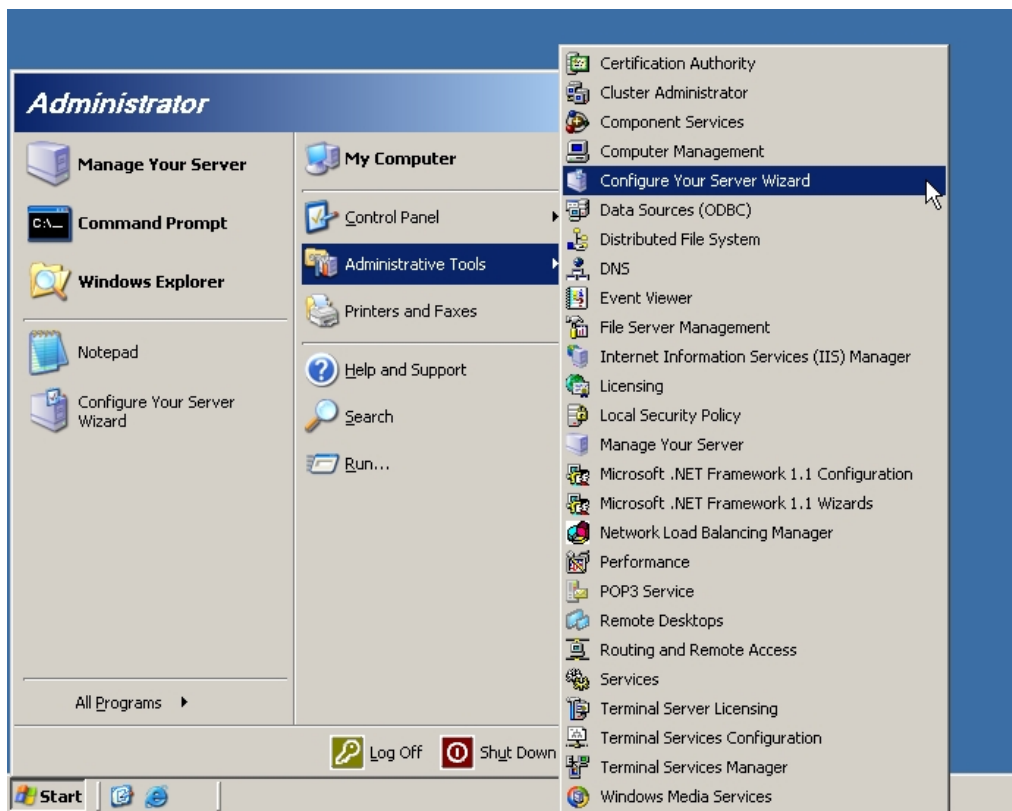
سرویس *Active directory*، فقط بر روی ویندوز سرور نصب می‌شود. جهت نصب این سرویس، احتیاج به یک IP استاتیک می‌باشد. در ضمن سرویس DNS باید بر روی شبکه موجود باشد (در غیر اینصورت، بطور اتوماتیک نصب خواهد شد).

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.

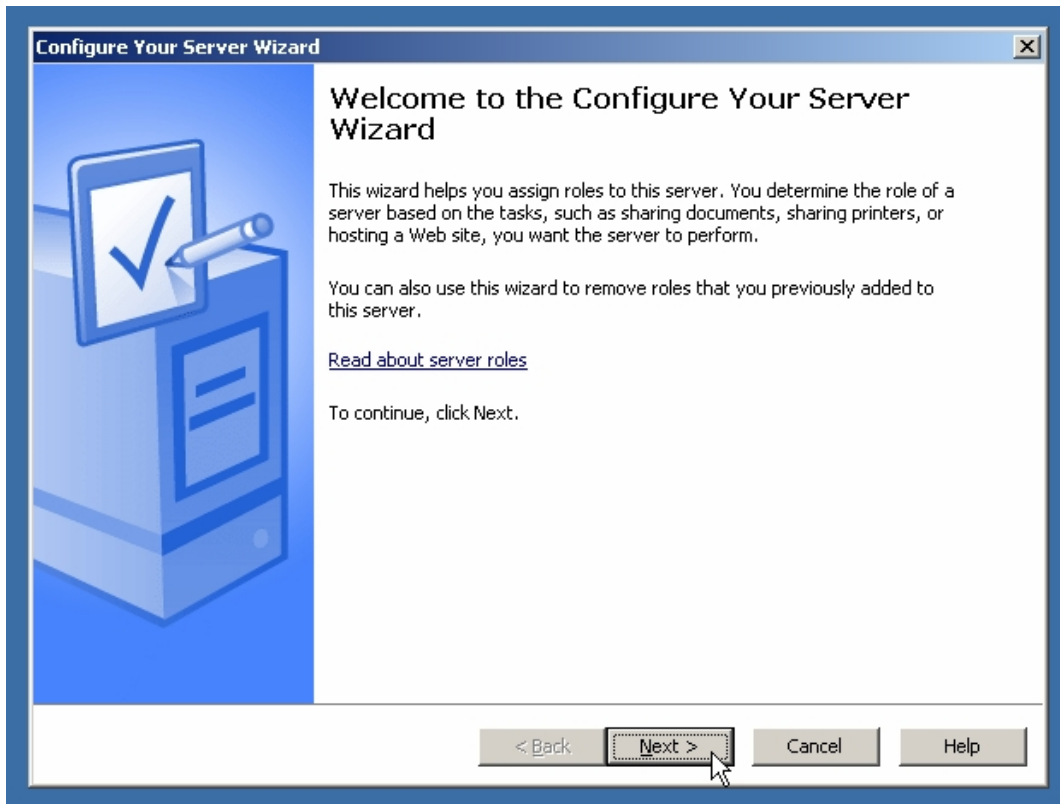
○ نحوه راه اندازی سرویس Active Directory

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

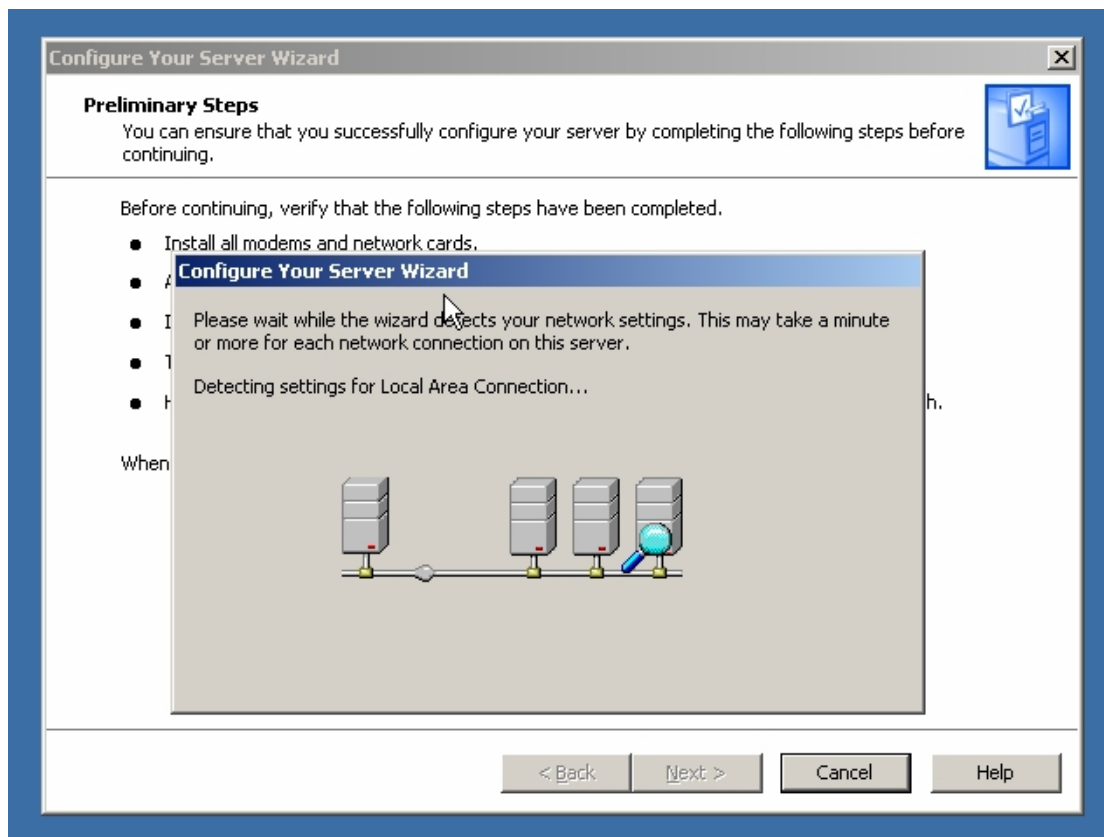
از منوی Start، بر روی گزینه Administrative Tools رفته و گزینه Configure Your Server Wizard را انتخاب کنید. منوی Administrative tools را می توانید در داخل Control panel نیز پیدا کنید.



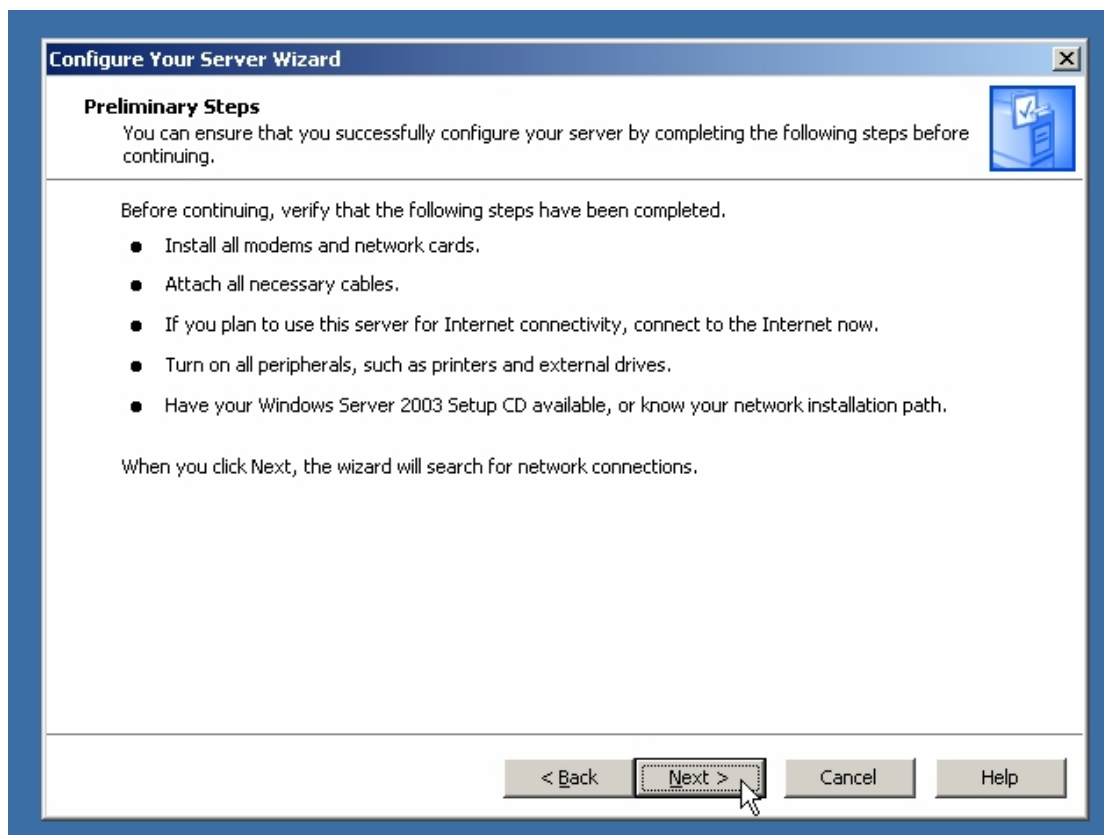
سپس از پنجره ظاهر شده گزینه Next را انتخاب کنید.



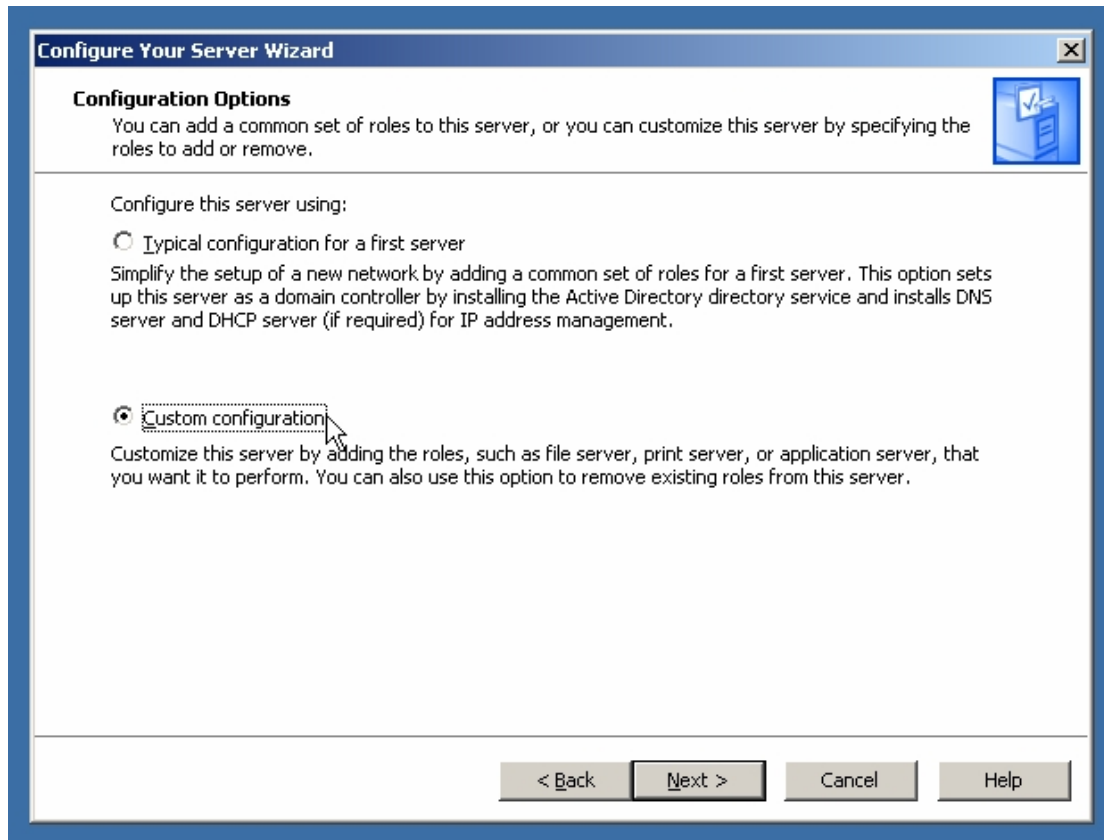
پنجره‌ای ظاهر شده و ترکیب فعلی شبکه بررسی می‌شود. در این قسمت وجود یا عدم وجود یک Domain Controller در شبکه نیز تعیین می‌شود.



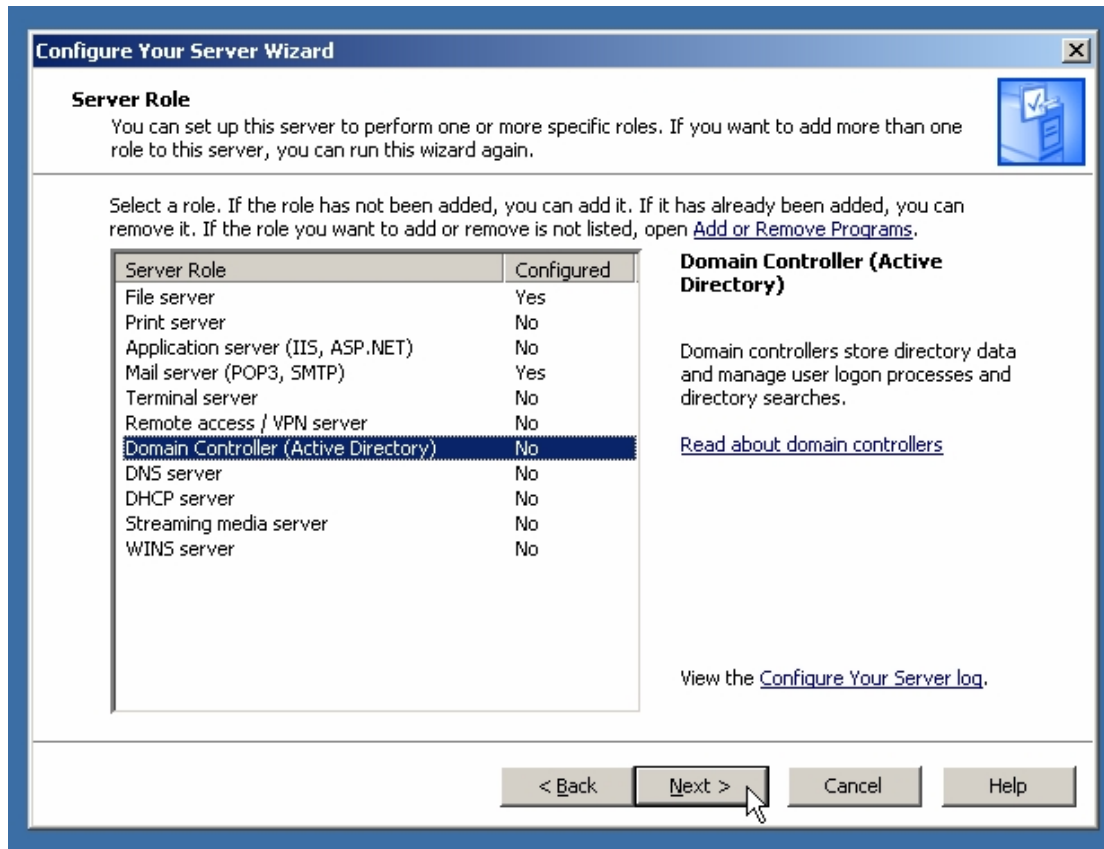
در پنجره بعدی، توصیه‌هایی در مورد نصب کامل کلیه سخت‌افزارهای کامپیوتر می‌شود. در این قسمت نیز گزینه Next را انتخاب کنید.



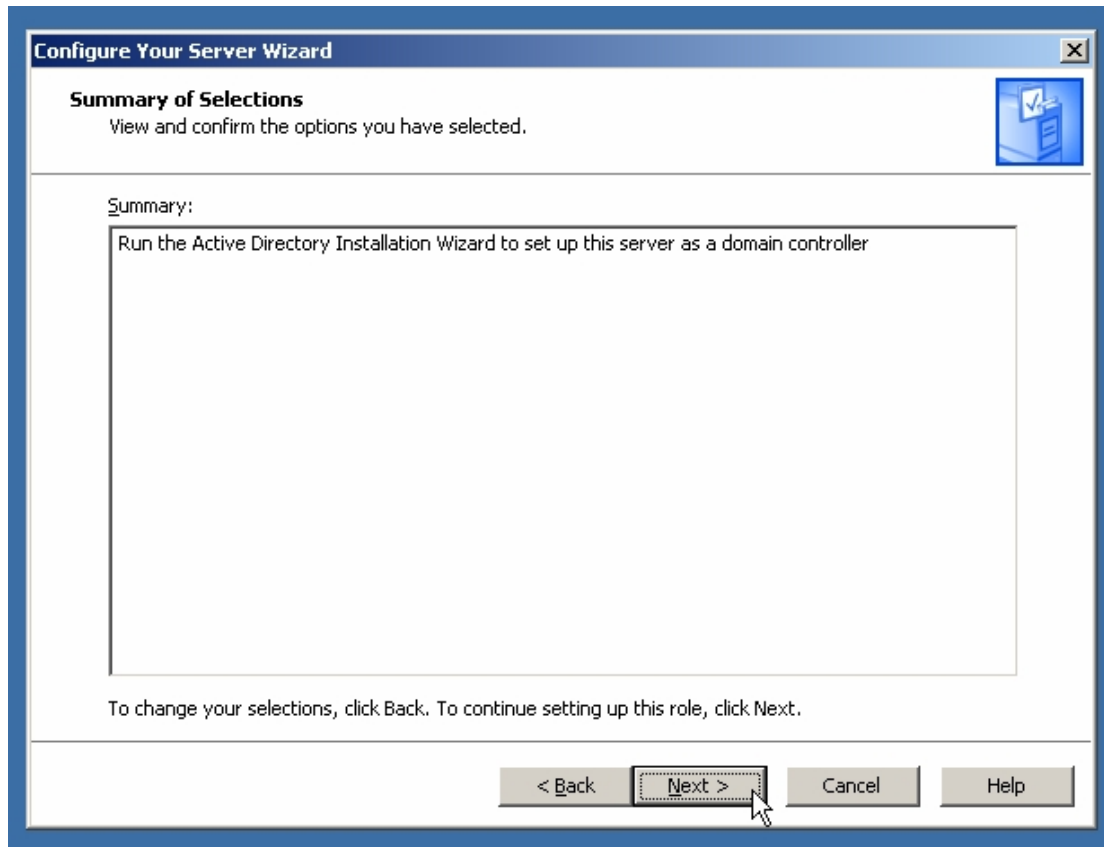
سپس گزینه Custom configuration را انتخاب کنید و دکمه Next را بزنید.



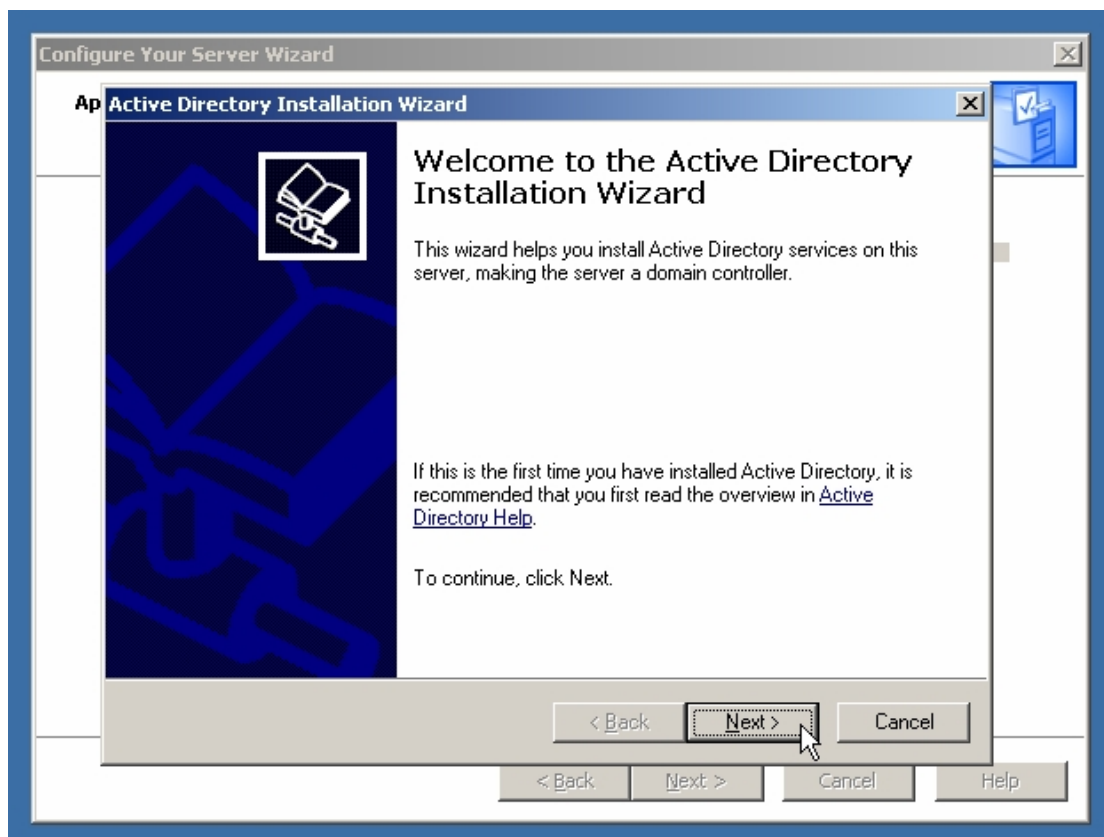
در این پنجره، می‌توان وظایف مختلفی را برای کامپیوتر (سرور خود) تعریف کرد. وظیفه‌ای که ما می‌خواهیم بر عهده سرور خود قرار دهیم، وظیفه Domain controller شبکه است. پس این گزینه را از داخل لیست انتخاب کنید و دکمه Next را بزنید.



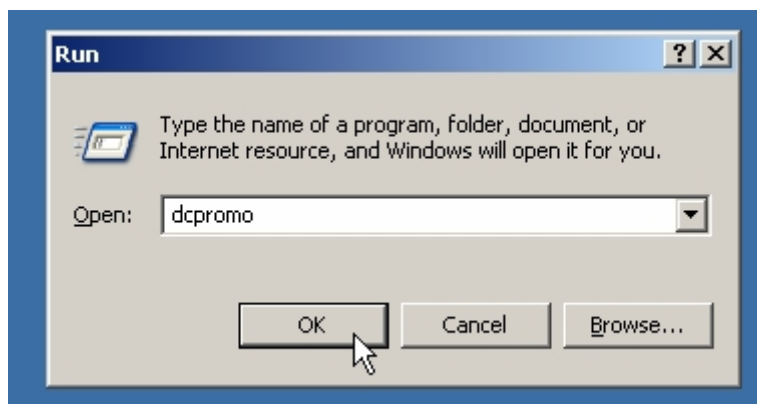
در پنجره بعدی نیز که خلاصه‌ای از اعمالی که باید انجام بگیرد را آورده است، دکمه Next را بزنید.



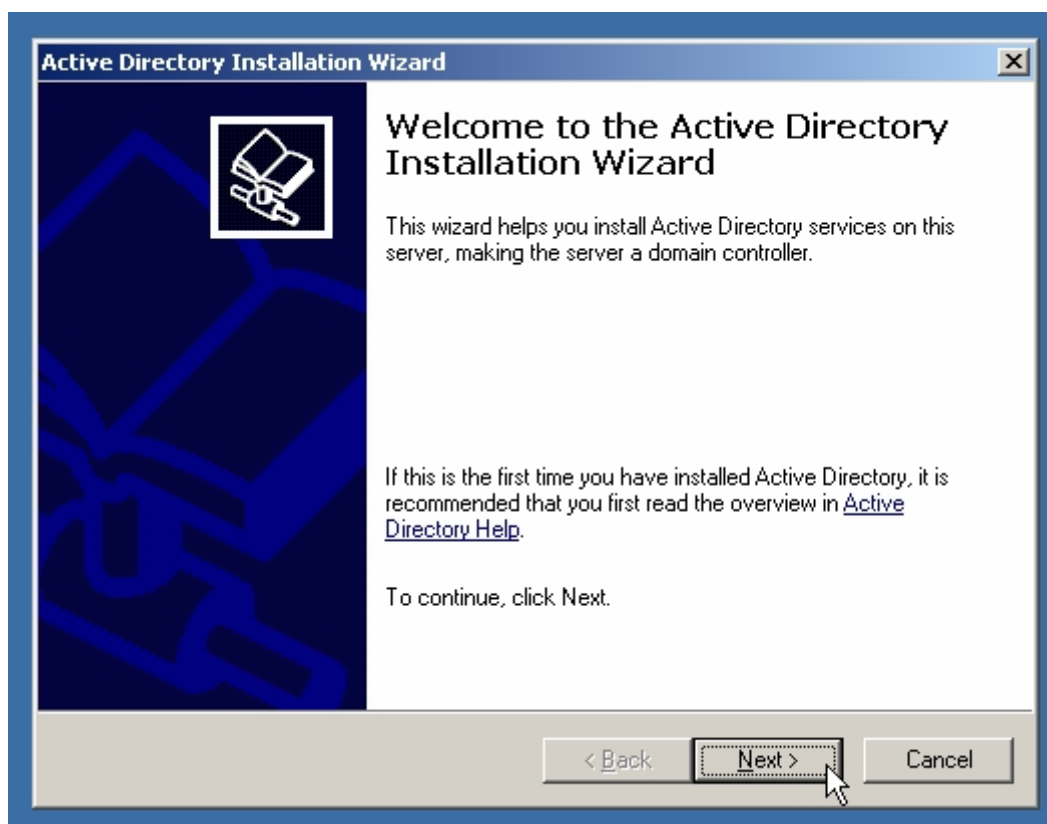
پس از زدن دکمه Next، مراحل نصب Active directory بر روی سرور آغاز می‌شود.
این مراحل در قسمت‌های بعدی توضیح داده می‌شود.



در روش دوم، از منوی Start گزینه Run را انتخاب کنید. سپس کلمه dcpromo را تایپ کرده، دکمه Ok را بزنید.

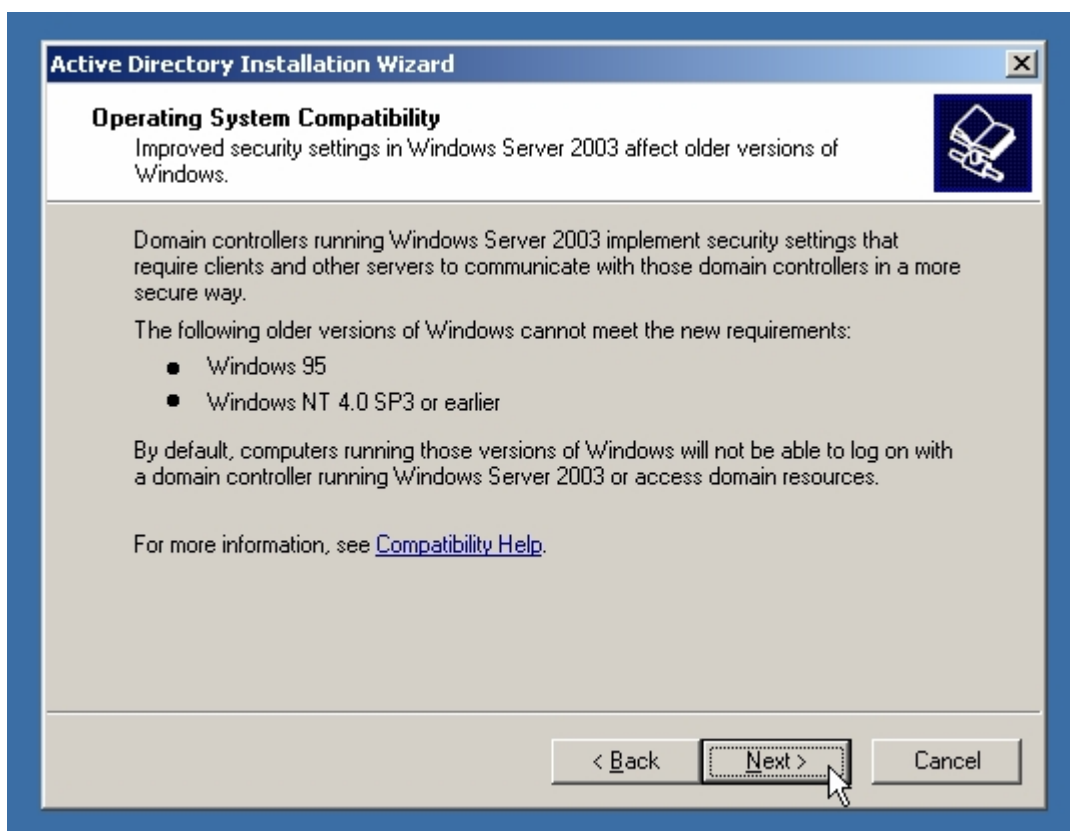


مانند روش اول، مراحل نصب Active directory شروع می شود.



○ نصب سرویس Active Directory

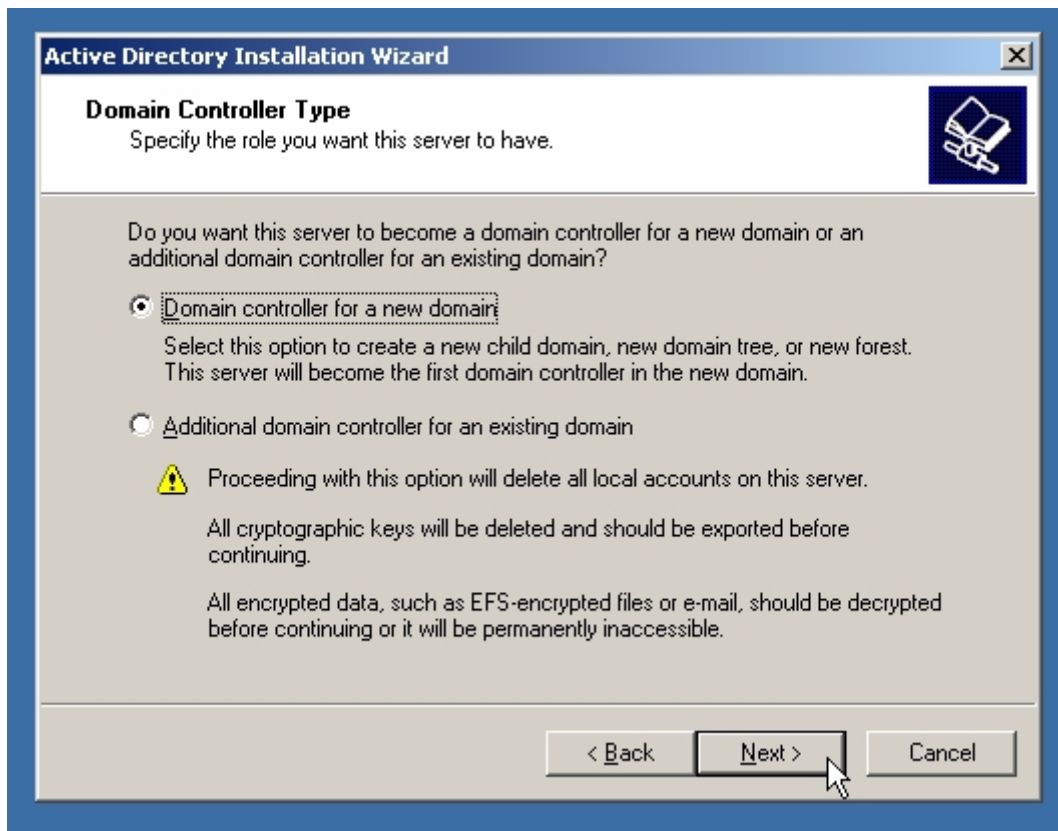
پس از فشار دادن دکمه Next پنجره زیر ظاهر می شود. در این پنجره بر این نکته تاکید می شود که کامپیوترهایی که دارای سیستم عامل های windows 95 و windows NT با 4 service pack 3 یا قدیمی تر هستند، نمی توانند عضوی از شبکه های ویندوز ۲۰۰۳ باشند. دلیل این امر، نوع تنظیمات حفاظتی است که در سرورهای ۲۰۰۳ وجود دارند و با نسخه های قدیمی ویندوز سازگار نیست.



نخستین سوالی که هنگام نصب Active directory پرسیده می‌شود، نحوه عملکرد این سرور در شبکه است. سرور فعلی می‌تواند خود یک Domain controller برای یک Domain جدید باشد، یا اینکه می‌تواند به عنوان یک Domain controller پشتیبان برای یک Domain موجود، عمل کند.

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

گزینه 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 است تعریف کنیم. در صورت از کار افتادن Domain controller، این سرور بطور خودکار وظیفه سرویس دهی به شبکه را بعهده می‌گیرد.



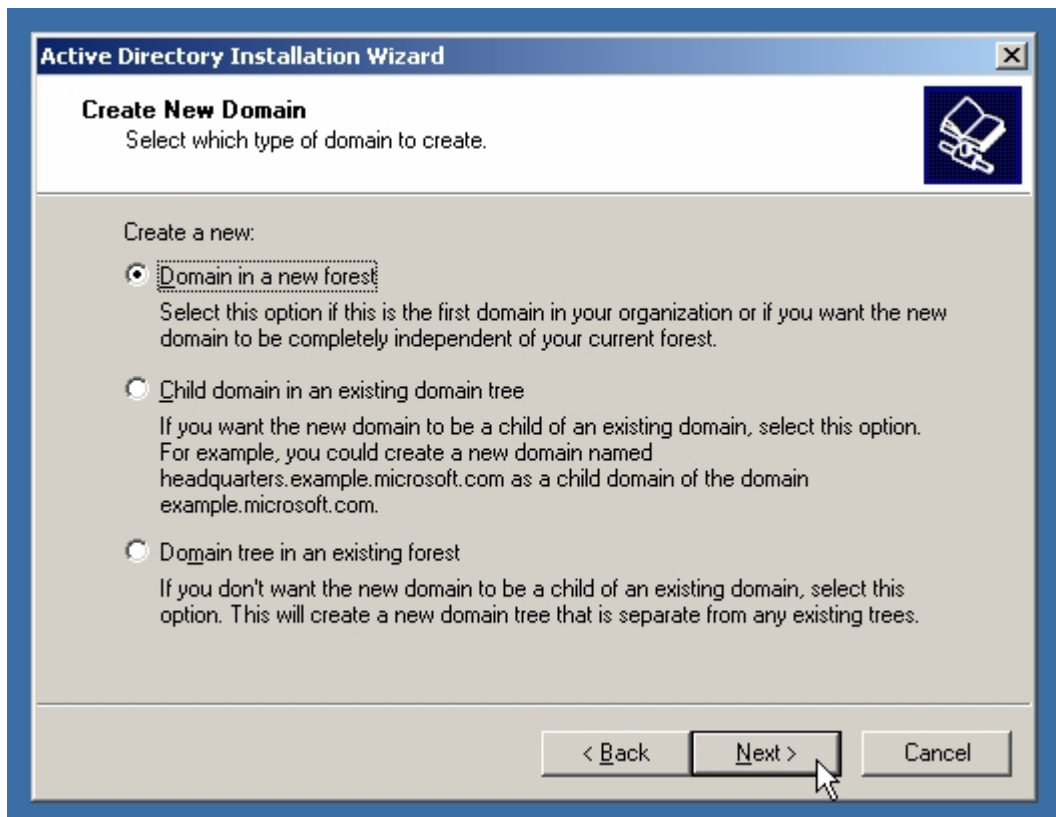
Domain جدید ما می تواند به سه صورت وجود داشته باشد. این Domain می تواند بطور کاملا مستقل ایجاد شود و به همین صورت کاملا مستقل فعالیت نماید.

در حالتی دیگر ، این Domain می تواند به زیر مجموعه Domain دیگری که Domain پدر نامیده می شود، 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.

گزینه سوم، سرور ما را تبدیل به یک Domain controller پدر که به آن می توانند، Domain های دیگر، متصل شوند، می کند.

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

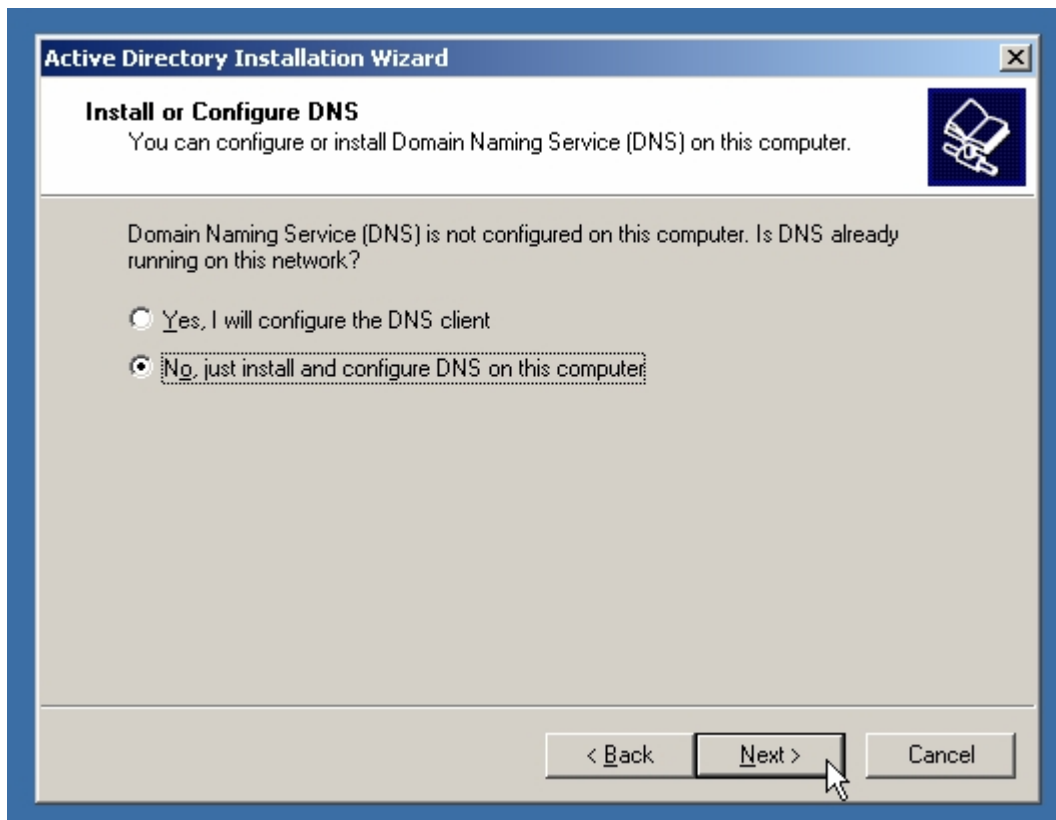
در این کلاس، ما به یک Domain کاملا مجزا نیاز داریم. به همین دلیل، گزینه اول را که پیش فرض نیز می باشد انتخاب کرده و دکمه Next را می زنیم.



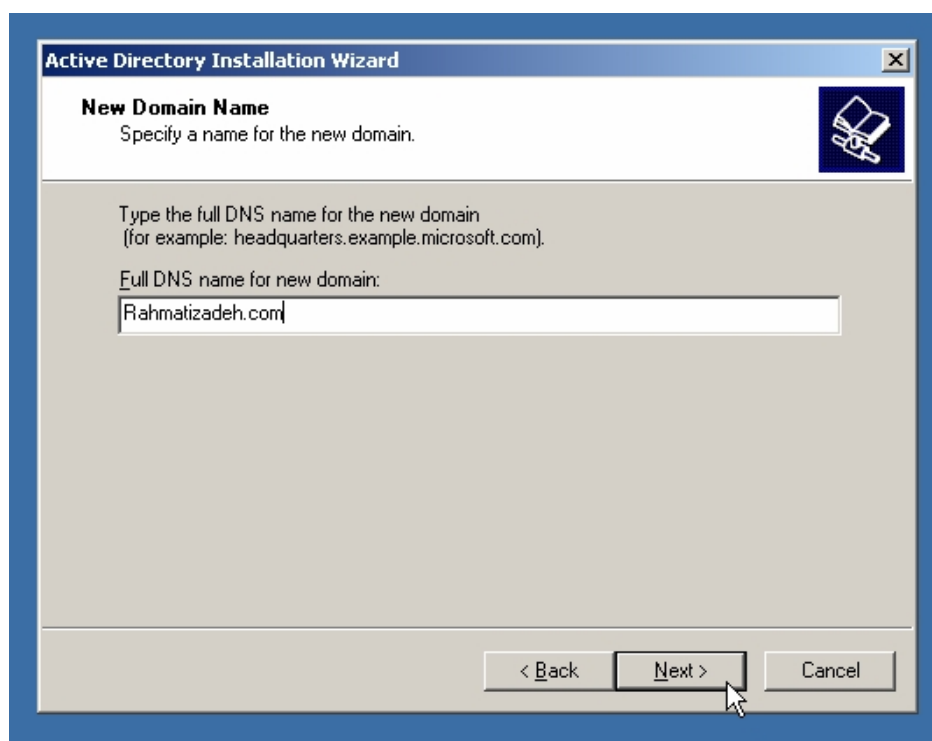
همانطور که در ابتدای جزوه گفته شد، لازمه داشتن سرویس Active directory، فعال بودن سرویس DNS در شبکه است. به همین دلیل در مرحله بعدی این سوال پرسیده می شود که آیا سرویس DNS در شبکه ما وجود دارد یا نه. در صورتیکه این سرویس در شبکه وجود داشته باشد، گزینه اول و در غیر اینصورت گزینه دوم را باید انتخاب کنیم.

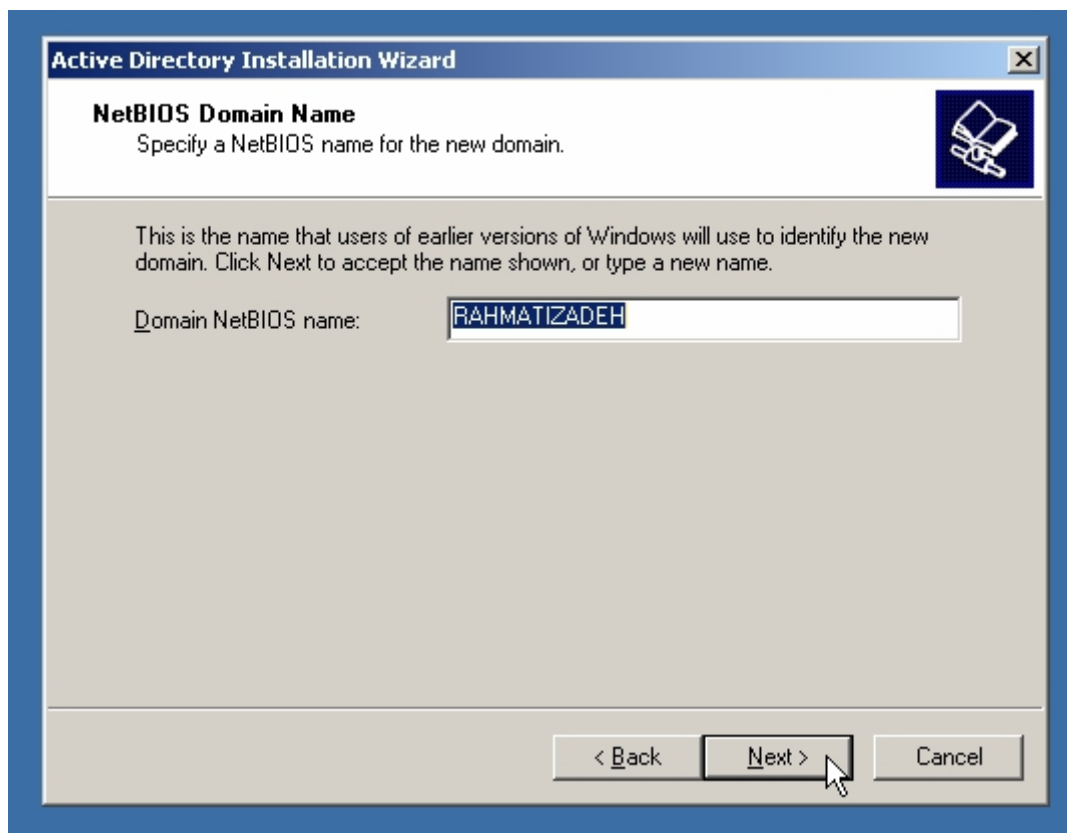
گزینه دوم، سرویس DNS را بر روی سرور ما نصب و راه اندازی می کند.

در این کلاس نیز با توجه به اینکه این سرور اولین سروری است که در شبکه راه اندازی می شود، گزینه دوم را انتخاب می کنیم و دکمه Next را می زنیم.

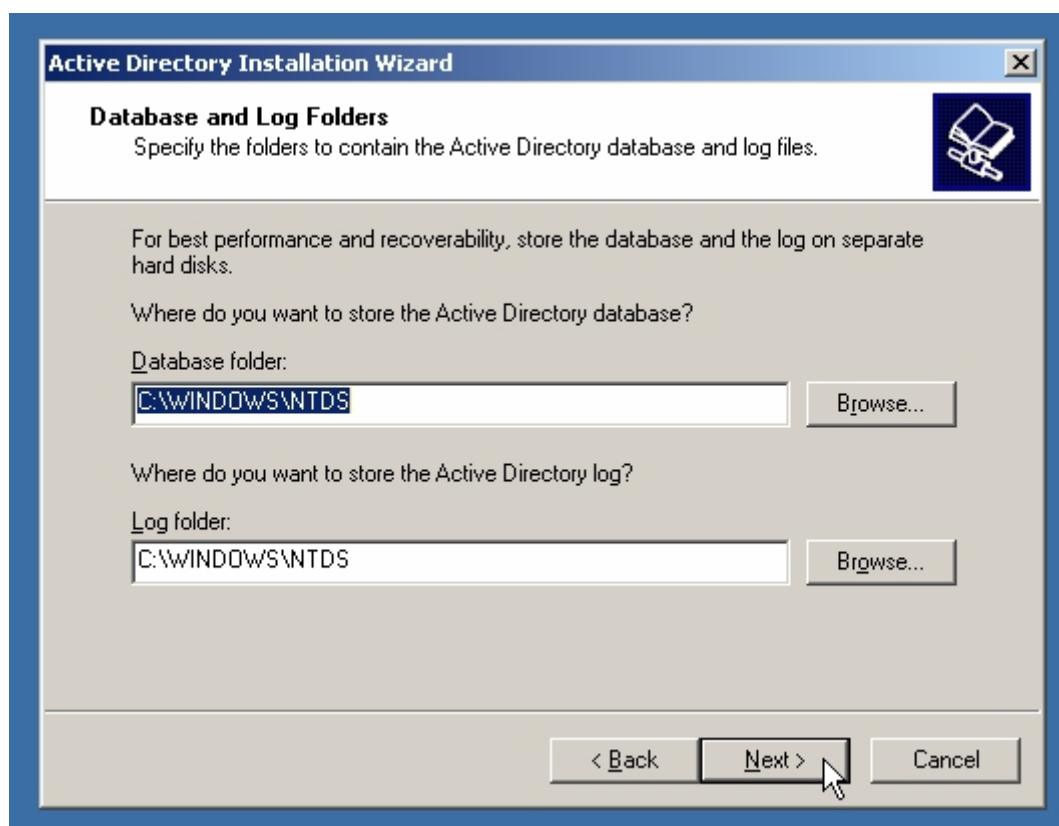


در مرحله بعدی نام Domain از ما خواسته می شود. این نام می تواند یک نام ثبت شده در اینترنت و یا غیره باشد. در پنجره اول نام کامل که شامل پسوند نیز می باشد را وارد می کنیم و در پنجره دوم، نام را بدون هیچ پسوند وارد می کنیم. دومین نام جهت استفاده در سیستم عامل های قدیمی مانند windows 98 می باشد.

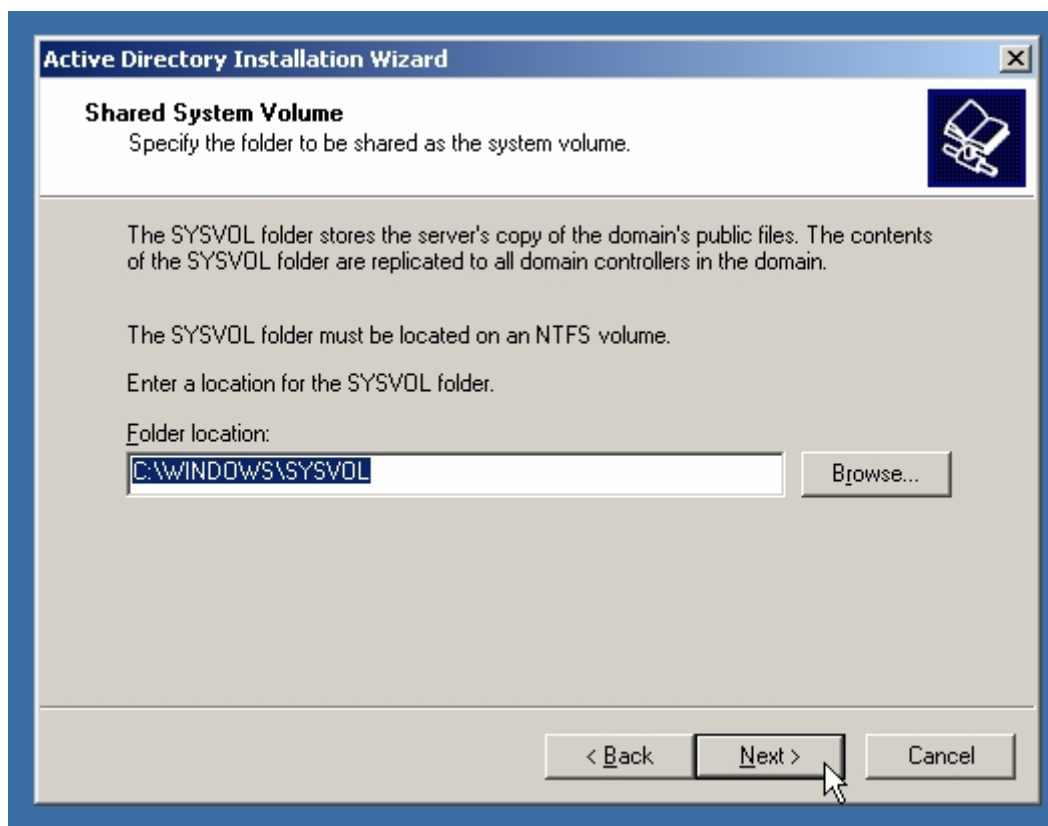




سپس مسیری را که در آن فایل‌های بانک Active directory قرار می‌گیرد را مشخص می‌کنیم. در این مثال مسیر پیشنهادی را انتخاب کنید.



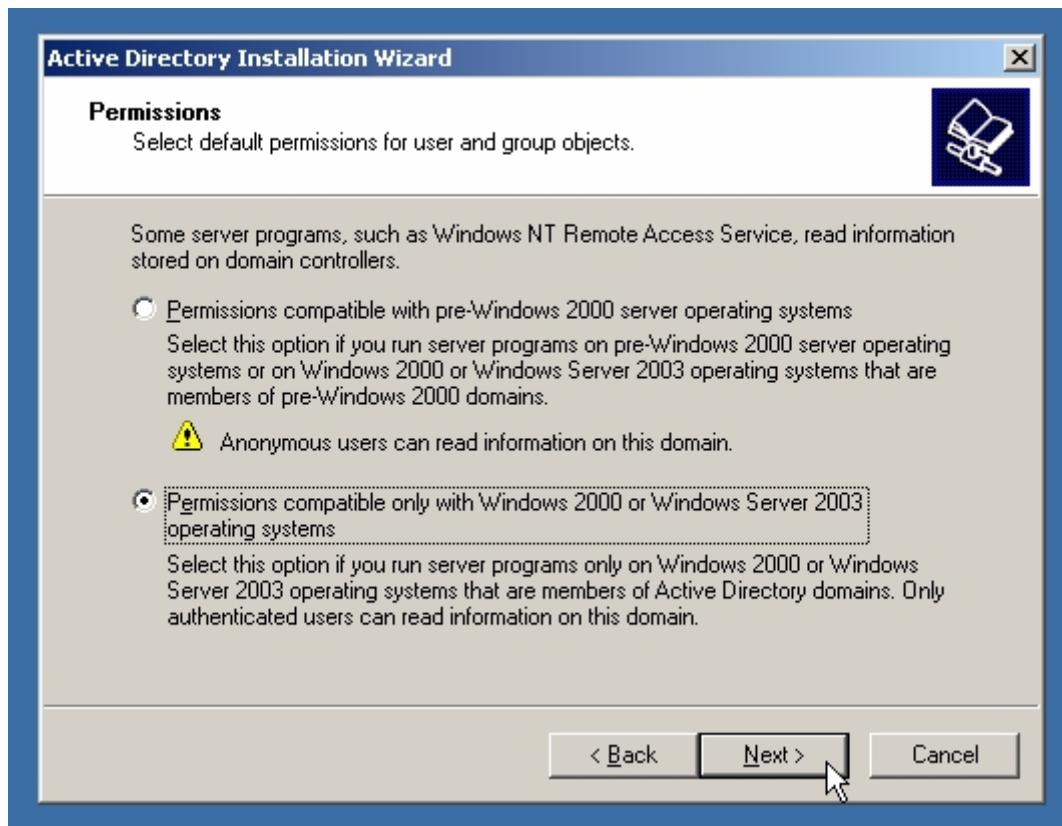
در هر domain controller، شاخه‌ای وجود دارد که اطلاعات عمومی شبکه بر روی آن قرار می‌گیرد. این شاخه در شبکه به اشتراک گذاشته می‌شود و اطلاعات موجود بر روی آن، بطور اتوماتیک بر روی domain controllerهای دیگر، تکثیر می‌شود. مسیر این شاخه در این قسمت پرسیده می‌شود. این شاخه باید بر روی NTFS ساخته شود.



رکوردهایی که در Active directory ساخته می‌شوند، باید قابل خواندن توسط برنامه‌های مختلف باشند. در نسخه‌های قدیمی ویندوز سرور مانند NT 4، کاربران بدون در نظر گرفتن دسترسی‌های تعیین شده، می‌توانستند به اطلاعات موجود در directory دسترسی داشته باشند. در سرورهای ۲۰۰۰ به بعد، هر کاربر فقط در صورت مجاز بودن می‌تواند به اطلاعات دسترسی داشته باشد.

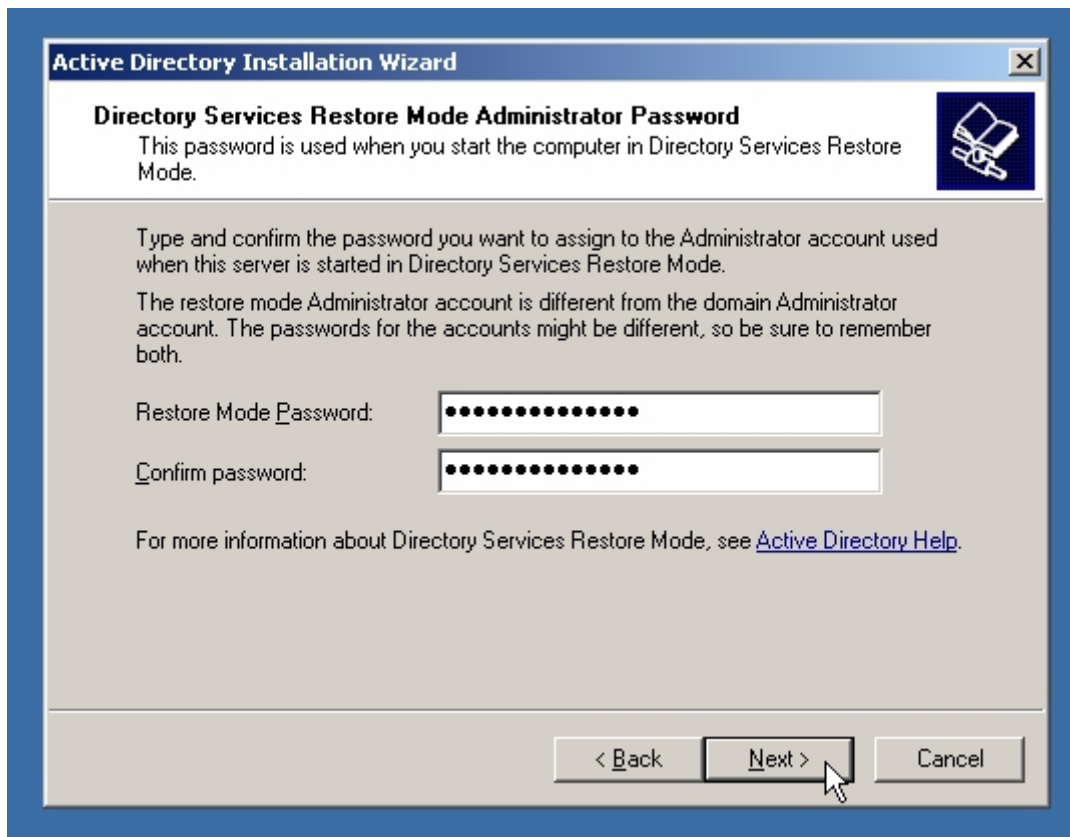
به همین دلیل، در صورتیکه در شبکه ما سرورهای قدیمی وجود داشته باشد، این عدم هماهنگی مشکل بوجود خواهد آورد. برای رفع این مشکل، سرویس Active directory به دو صورت می‌تواند فعالیت کند. یا بصورتیکه قابل استفاده به همراه سرورهای قدیمی‌تر باشد (که حفاظت کمتری دارد) یا در حالتیکه در شبکه فقط سرورهای ۲۰۰۰ و ۲۰۰۳ وجود دارند (که حفاظت بالاتری دارد).

در این مثال، ما گزینه دوم را که پیش‌فرض نیز می‌باشد انتخاب می‌کنیم و دکمه Next را می‌زنیم.

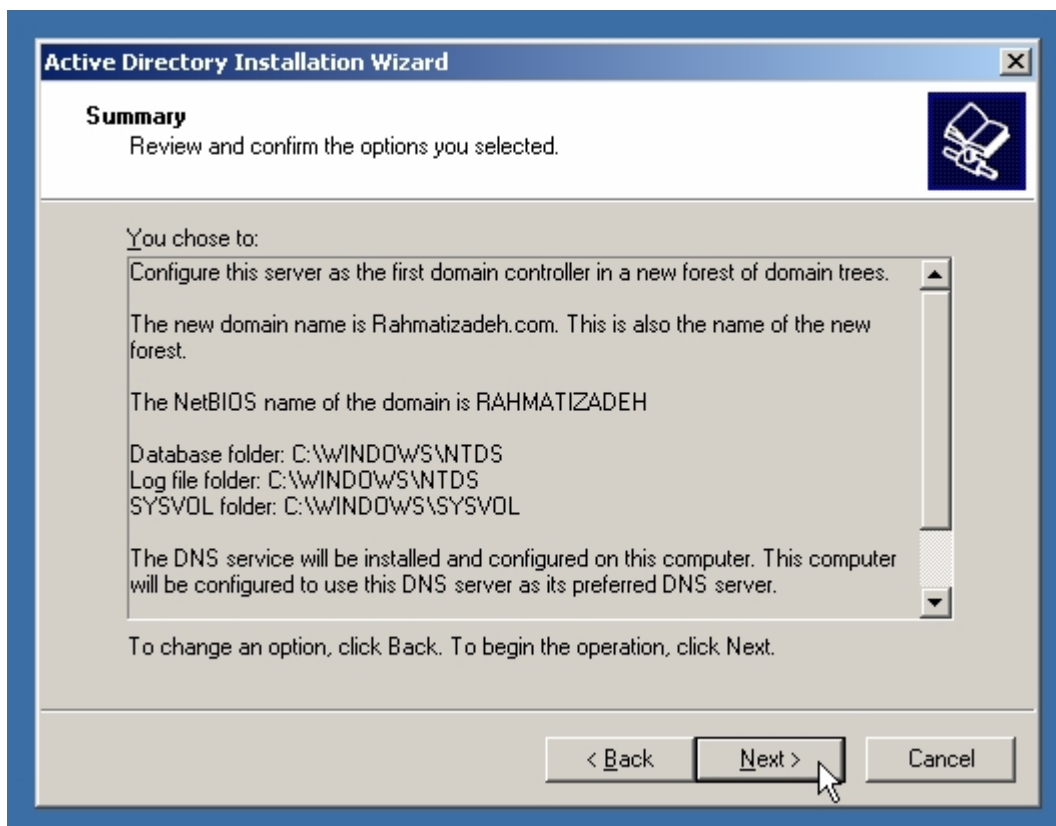


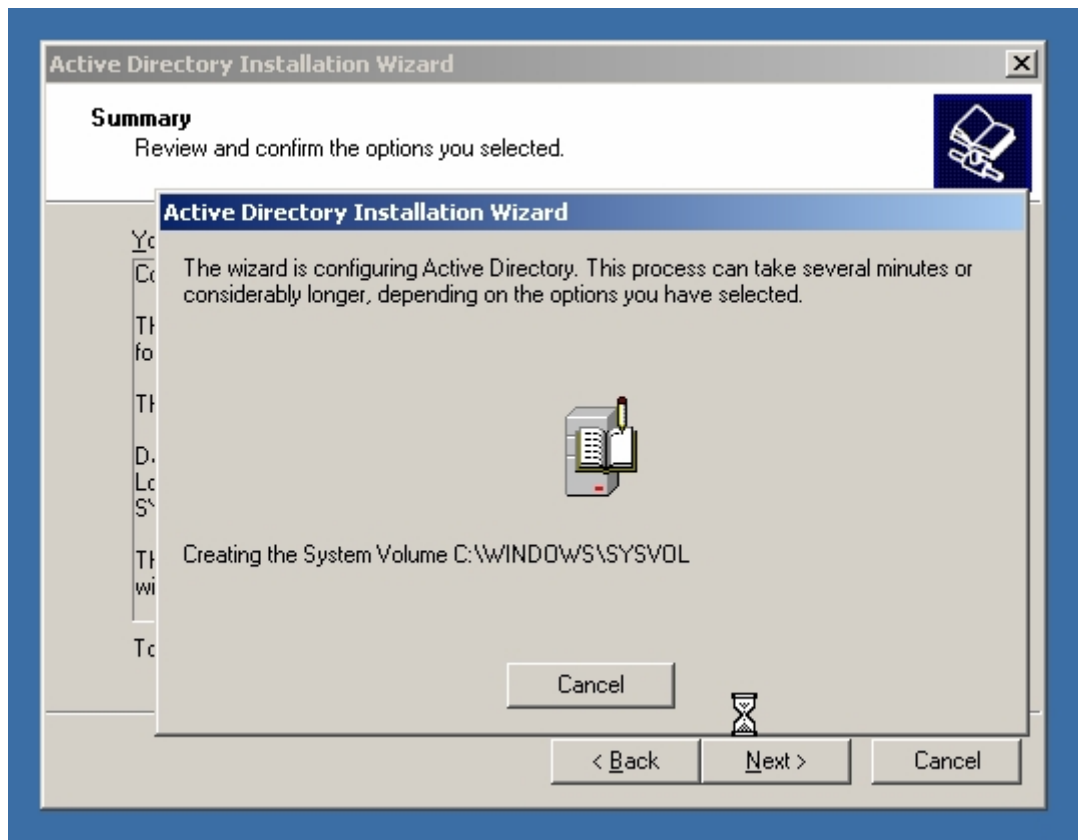
کلیه اطلاعات مربوط به کاربران مختلف در Active directory نگه داشته می شود. اطلاعات مربوط به Administrator شبکه نیز به همین صورت است. در صورتیکه برای فایل های Active directory مشکلی بوجود آید، اطلاعات مربوط به کاربران از بین خواهد رفت. در domain controller ها در هنگام بالا آمدن سیستم عامل و با زدن کلید F8، گزینه ای تحت عنوان Directory Services Restore Mode وجود دارد، که این امکان را می دهد 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 جداگانه ای برای این مرحله از کاربر پرسیده می شود. در این قسمت ما این رمز را تعیین می کنیم.

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

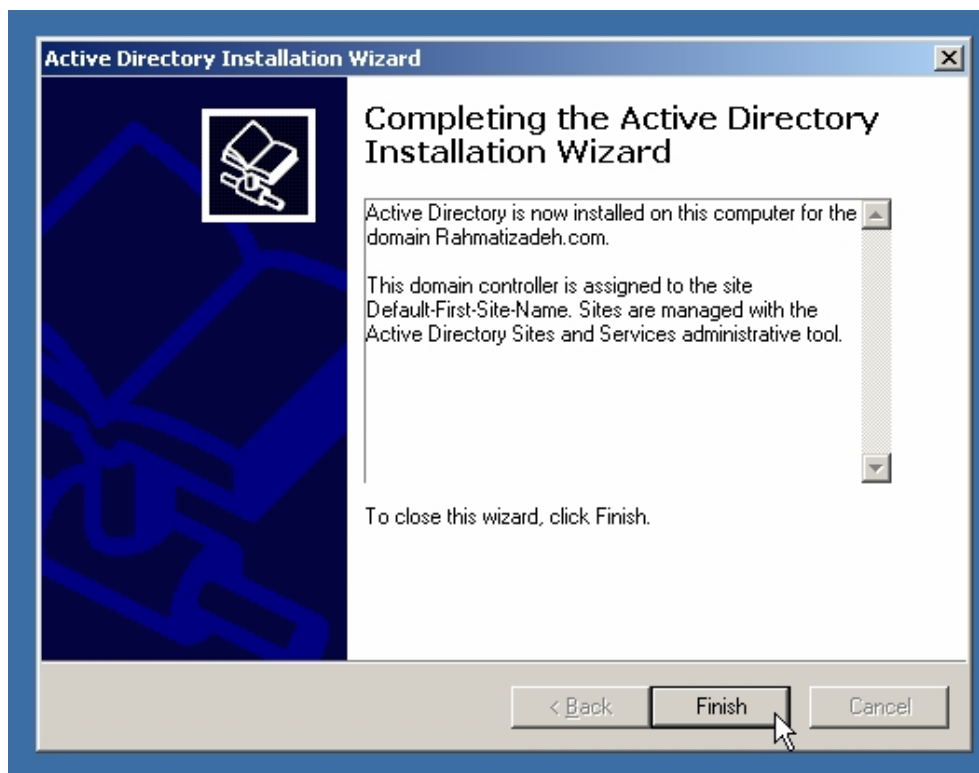


در انتها، خلاصه‌ای از موارد وارد شده توسط کاربر نشان داده می‌شود. پس از زدن کلید Next، نصب Active directory بر روی سرور آغاز می‌شود.





پس از پایان، در صورت موفقیت آمیز بودن نصب Active directory پنجره زیر نمایش داده خواهد شد. پس از زدن دکمه 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 controller ها نمی‌توان خارج از شبکه لاگین کرد.



Object های استاندارد موجود در Active Directory

از Object های مختلفی که در Active directory وجود دارد، در کلاس شبکه مبتدی، فقط به Object های خاص می‌پردازیم: Organizational Unit ها مانند folder ها وظیفهٔ تقسیم‌بندی در Active directory را برعهده دارند. با استفاده از OU ها، مدیر شبکه می‌تواند Object های دیگر را بصورت منطقی از هم جدا کند. معمولاً این جداسازی به سه منظور انجام می‌شود: ۱- جداسازی ظاهری جهت تقسیم‌بندی ظاهری و برای راحتی شدن کار با Object ها ۲- جداسازی به منظور اعمال سیاست‌های مختلف بر روی یکدسته از Object های خاص ۳- مخفی‌سازی تعداد خاصی از Object ها در شبکه.

در کلیه حالت‌های ذکر شده، OUها مانند folderها که وظیفه 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، وظیفه 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.

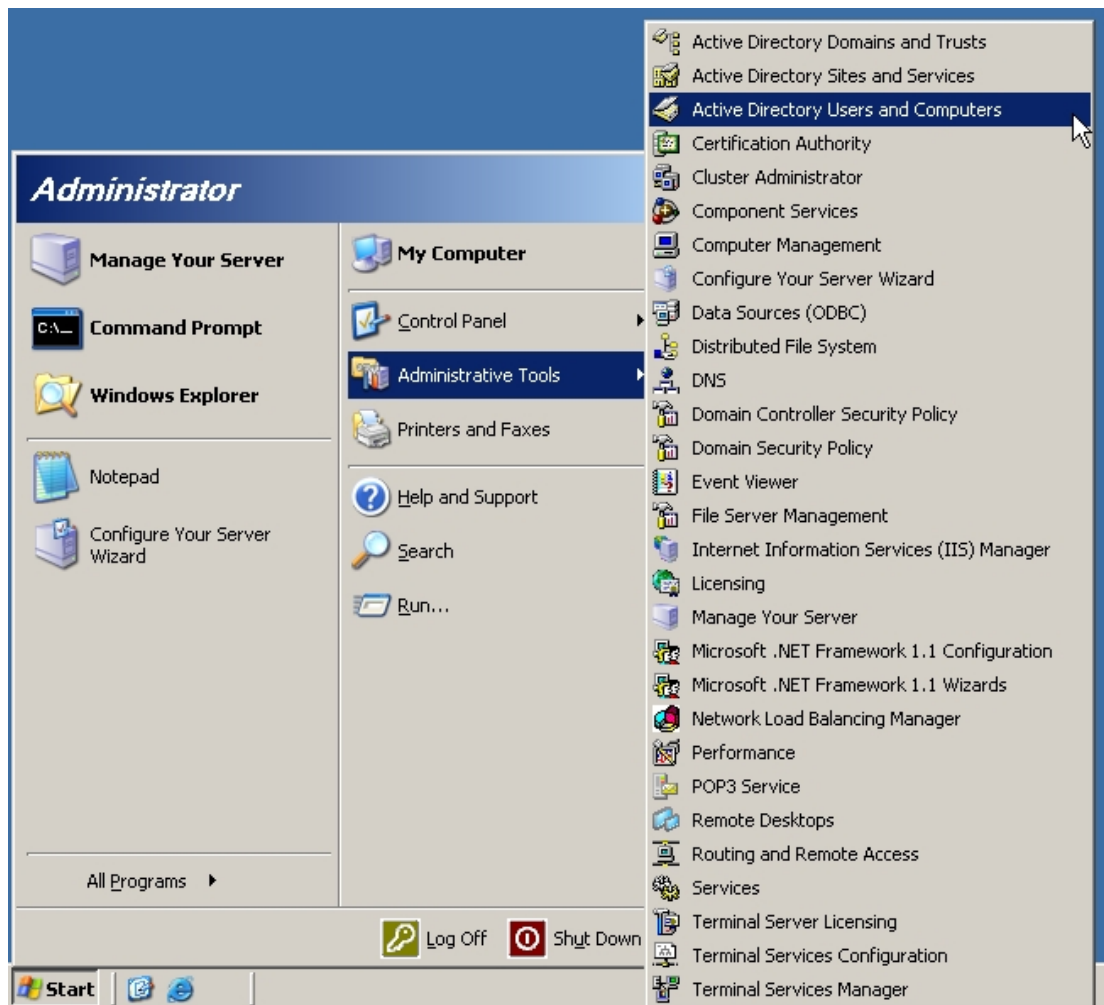
Groupها، جهت دسته‌بندی کاربران و کامپیوترهای موجود در شبکه استفاده می‌شوند. مدیر شبکه می‌تواند برای سهولت کار خود، کاربران و کامپیوترها را در گروه‌های منطقی قرار دهد. برای مثال، مدیر شبکه می‌تواند دو گروه "کاربران عادی" و "کاربران خاص" را تعریف کند. سپس کاربران موجود در Active directory را به عضویت این گروه‌ها در آورد 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 گروه که همه این کاربران عضو آن هستند، شرایط تعریف می‌شود.

○ نحوه مدیریت Active Directory

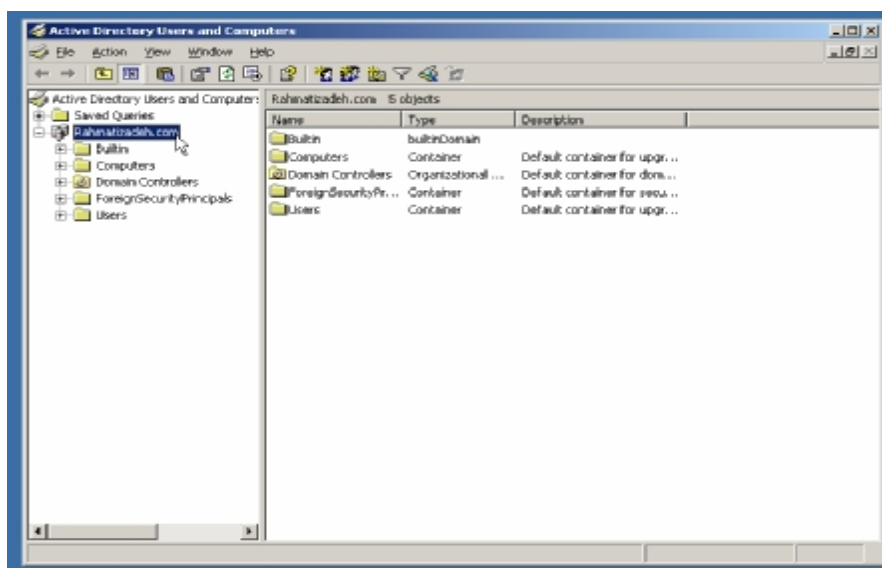
ابزارهای مختلفی جهت مدیریت Active directory در سرورهای ۲۰۰۳ وجود دارد. در این فصل به شرح تعدادی از این ابزارها می‌پردازیم:

§ 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 برنامه 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 به ترتیب برای نشان دادن تقسیم‌بندی‌های پیش‌فرض و OUها استفاده می‌شود:



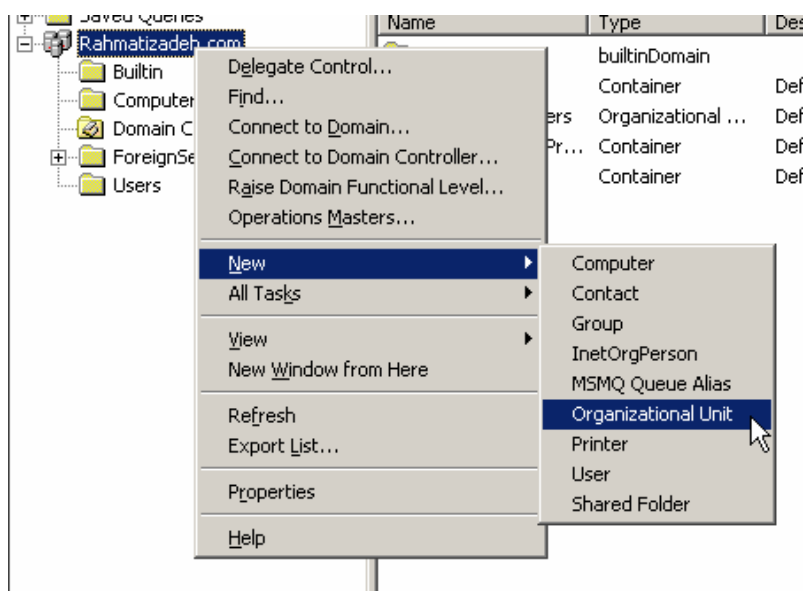
با انتخاب هر کدام از این تقسیم‌بندی‌ها، در قسمت سمت چپ، محتویات آن‌ها نشان داده می‌شود. هر کدام از objectهایی که در قبل گفته شد، دارای علامت خاصی در

Active directory users and computers هستند. از علامت  برای

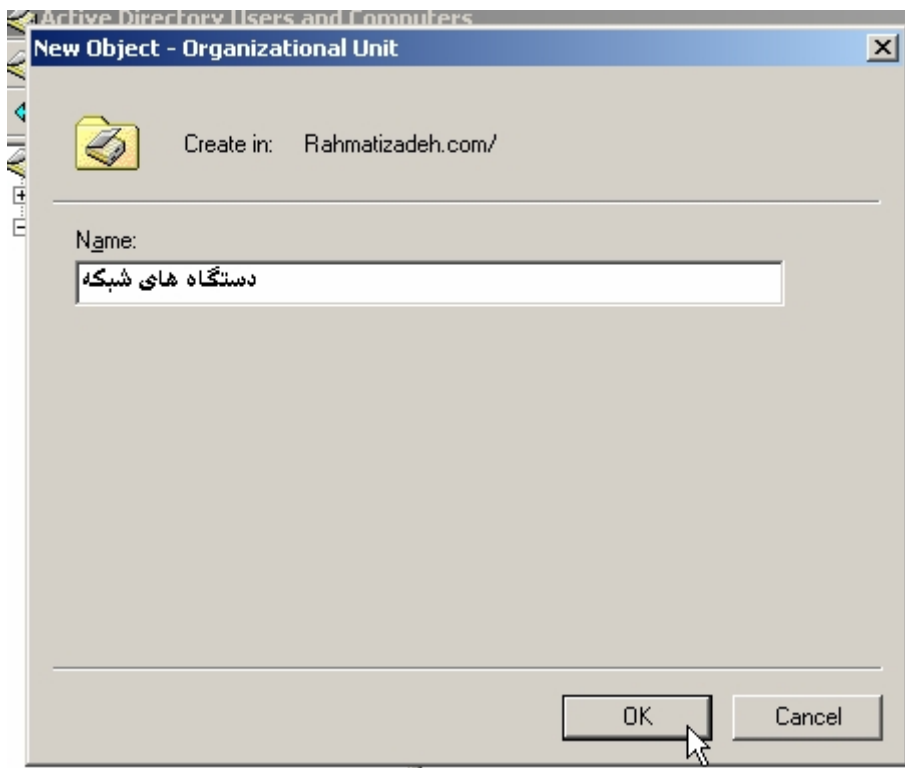
نمایش کامپیوترها، از  برای نمایش کاربران و از  برای نشان دادن گروه‌ها استفاده می‌شود.

§ Organizational Units

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



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



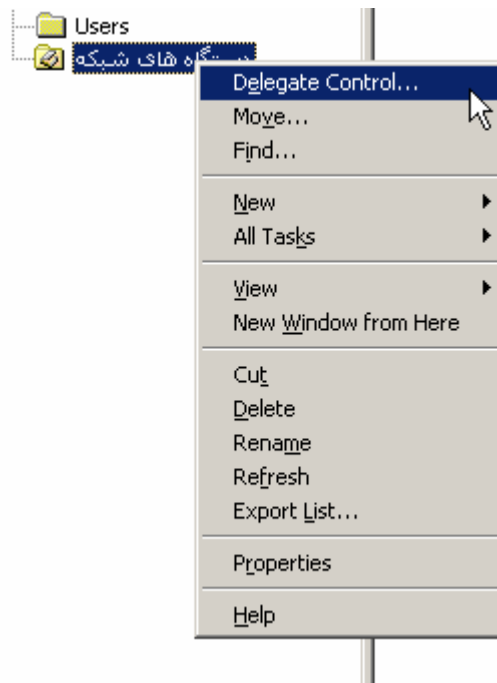
Organization Unit جدید ساخته می‌شود.



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 دکمه سمت راست موس، گزینه Move را انتخاب کنیم.

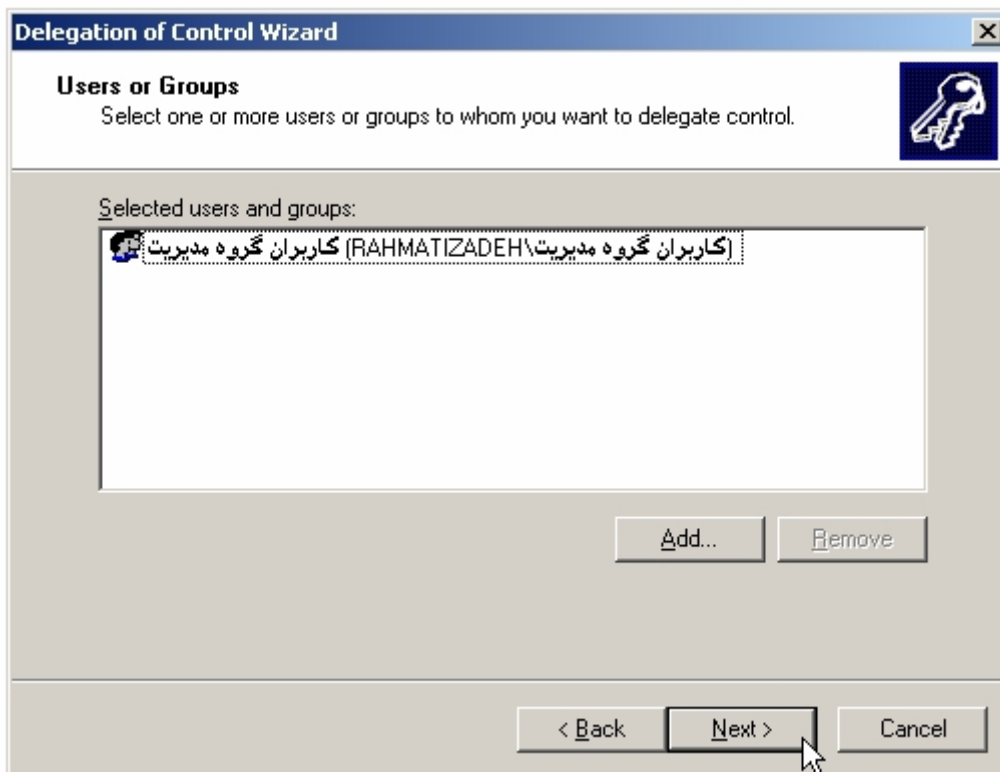
با استفاده از OUها می‌توان مدیریت objectهای داخل آنها را به شخص دیگری محول کرد. این امر به دو روش امکان‌پذیر است. در روش اول، با زدن دکمه سمت راست موس بر روی OU مورد نظر از منوی ظاهر شده، گزینه Delegate control را انتخاب می‌کنیم.



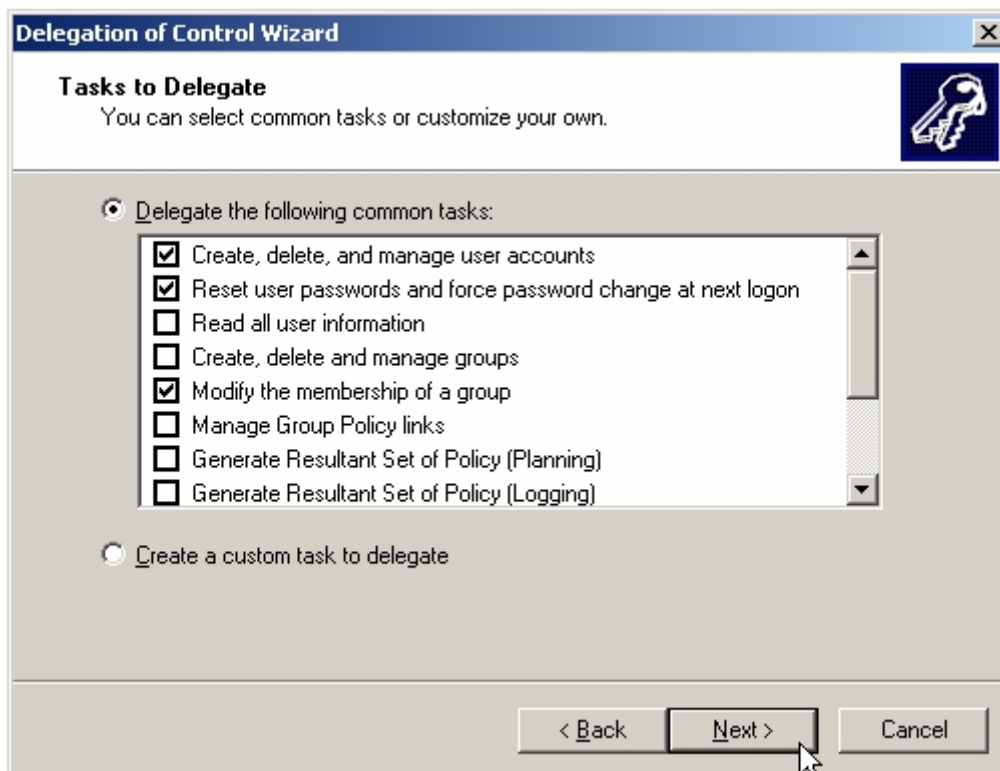
در اولین صفحه ظاهر شده، دکمه Next را انتخاب می‌کنیم.



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



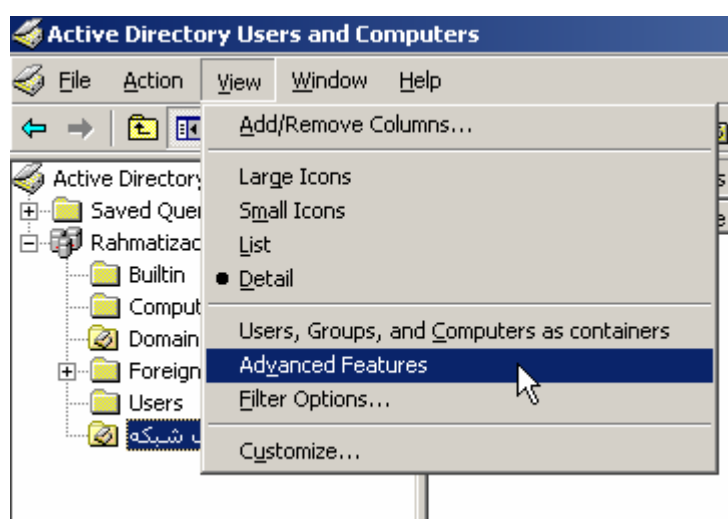
در پنجره بعدی از بین اعمال متداول و پیش فرض مدیریتی، اعمال پیش فرض را انتخاب می کنیم. در غیر این صورت می توان با انتخاب گزینه Create a custom task to delegate، به دلخواه اعمالی را تعریف کنیم.



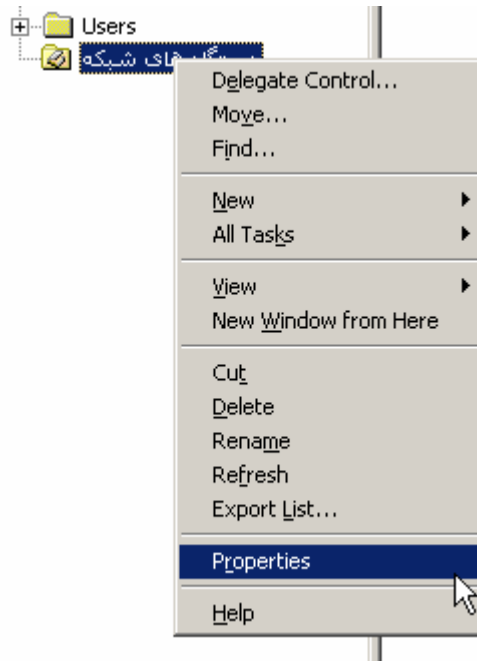
پس از زدن دکمه Finish، اعمال مدیریتی انتخاب شده، فقط برای objectهایی که درون این OU هستند، در کنترل کاربران یا گروه‌هایی که انتخاب کرده‌ایم درمی‌آیند.



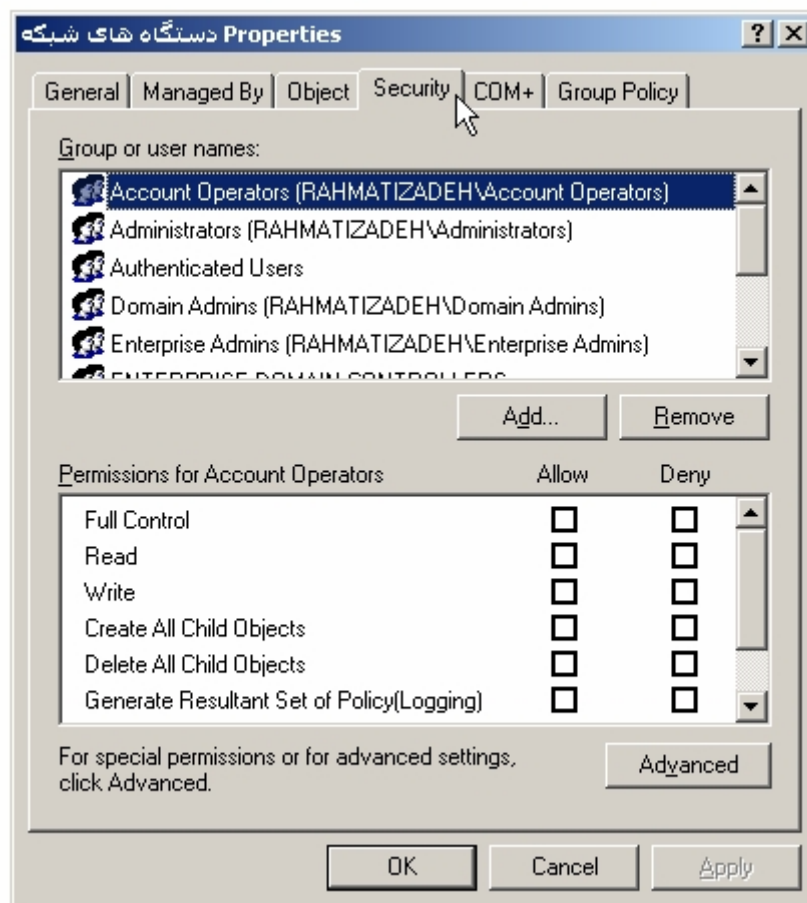
در روش دوم، ابتدا منوی view را باز کرده، گزینه advanced features را انتخاب می‌کنیم.



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



در پنجره ظاهر شده، سربرگ Security را انتخاب می‌کنیم. در لیست بالایی، نام کاربران یا گروه‌هایی را که می‌خواهیم اضافه می‌کنیم و در لیست پایینی، دسترسی‌های لازم را به هر کدام می‌دهیم.



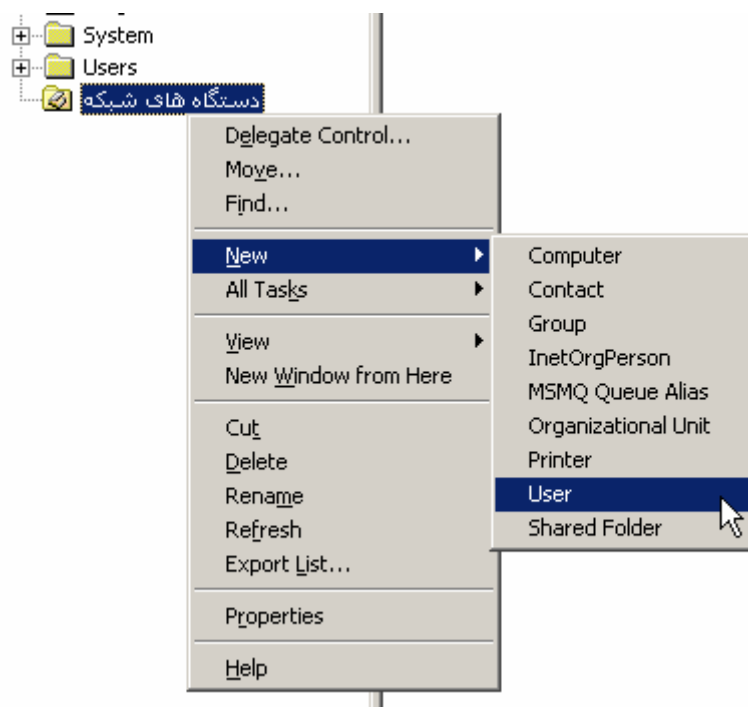
یکی دیگر از دلایل استفاده از OUها اعمال سیاست‌های خاص بر روی گروهی از Objectها می‌باشد. این Objectها را درون یک OU قرار داده و سیاست‌های خاص این OU را تعریف می‌کنیم. توضیحات کامل در مورد سیاست‌های شبکه، در قسمت Group policy داده می‌شود.

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 دکمه سمت راست موس را می‌زنیم. سپس از منوی باز شده گزینه New و سپس User را انتخاب می‌کنیم.



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

New Object - User

Create in: Rahmatizadeh.com/دستگاه های شبکه

First name: علیرضا Initials: []

Last name: رحمتی زاده

Full name: علیرضا رحمتی زاده

User logon name: Rahmatizadeh @Rahmatizadeh.com

User logon name (pre-Windows 2000): RAHMATIZADEH\ Rahmatizadeh

< Back Next > Cancel

در پنجره بعدی، رمز کاربر را دوبار وارد می کنیم. 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 هنگامی که کاربر رمز خود را عوض نکرده است، به وی اجازه کار نمی دهد. در صورتیکه بخواهیم امکان عوض کردن رمز را از کاربر بگیریم، گزینه User cannot change password و اگر بخواهیم اعتبار رمز کاربر تمام نشود (این گزینه در قسمت های بعدی به تفصیل توضیح داده خواهد شد)، گزینه Password never expires و اگر بخواهیم کاربر غیر فعال باشد (نتواند Login کند) گزینه account is disabled را انتخاب می کنیم. برای اتمام کار گزینه Next را می زنیم.

New Object - User

Create in: Rahmatizadeh.com/دستگاه های شبکه

Password: []

Confirm password: []

User must change password at next logon

User cannot change password

Password never expires

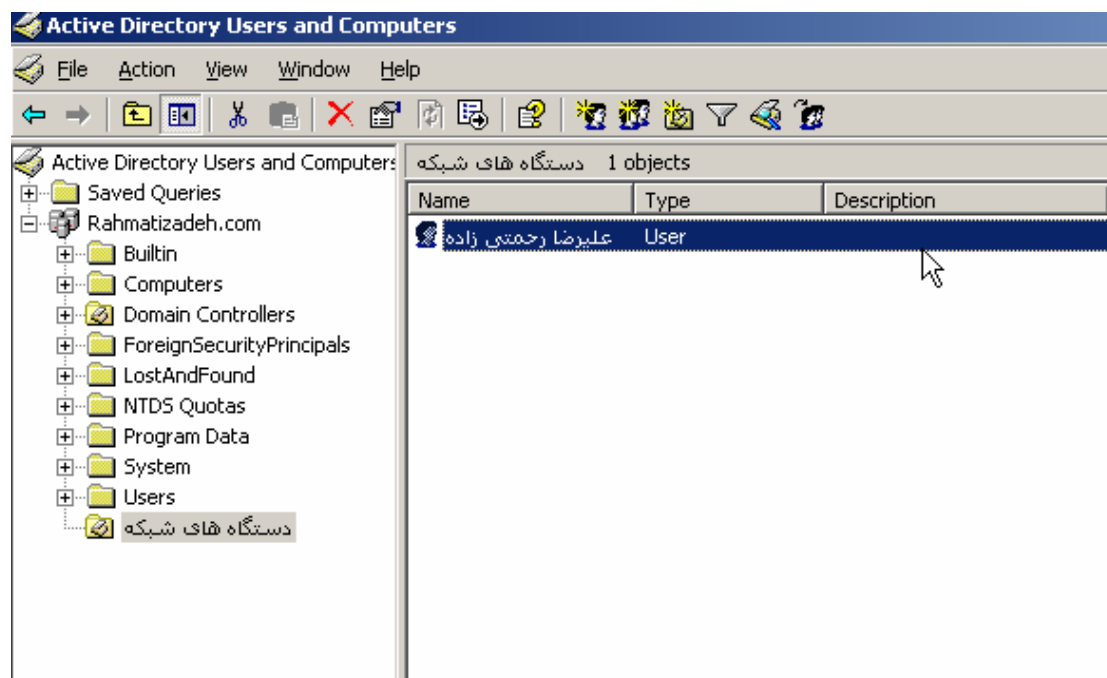
Account is disabled

< Back Next > Cancel

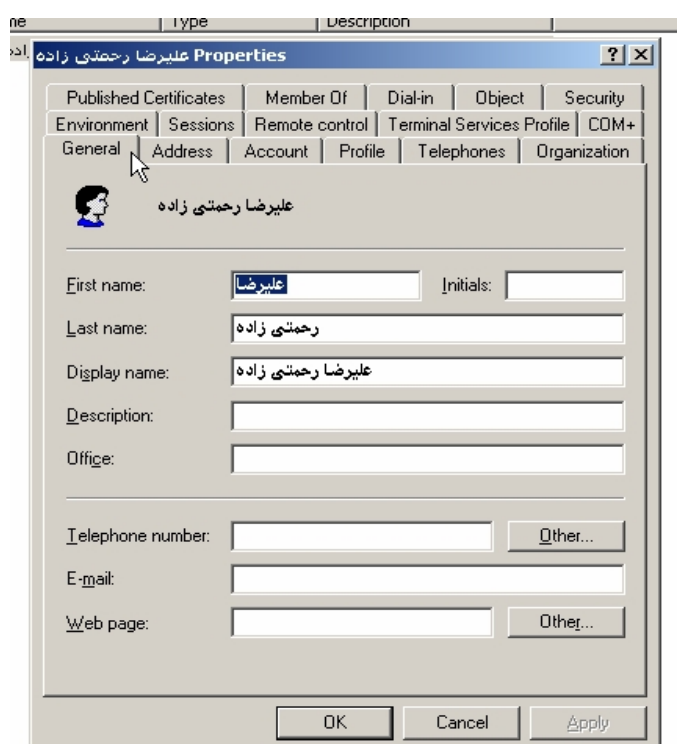
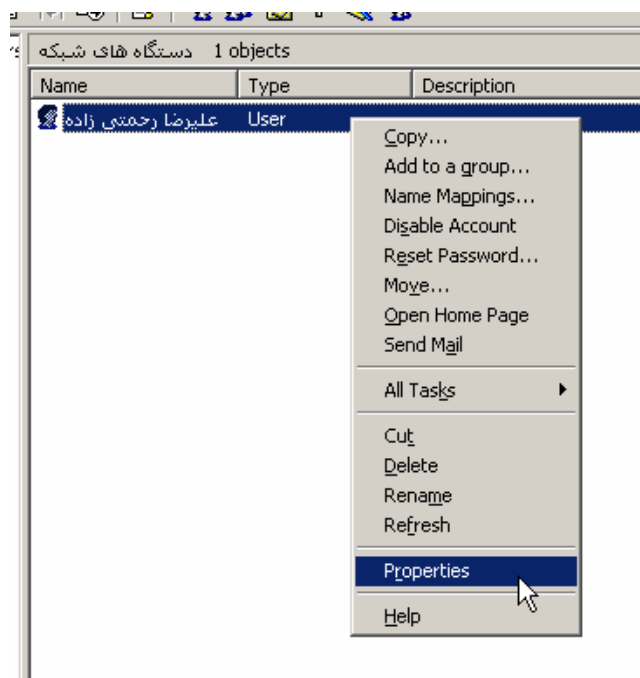
در آخرین پنجره خلاصه‌ای از آنچه انتخاب شده نمایش داده می‌شود. با زدن دکمه Finish کاربر جدید ساخته می‌شود.



اکنون کاربر علیرضا رحمتی زاده، 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 به عناوین ذکر شده نیست. اکنون اگر بر روی کاربر مورد نظر دکمه سمت راست موس را بزنیم و گزینه properties را انتخاب کنیم، اطلاعات کاملتری را در مورد هر کاربر می‌توانیم وارد کنیم (توجه داشته باشید که در تمرین‌های قبلی گزینه advanced features را از منوی view فعال کرده‌ایم)



قسمت‌های مختلف این پنجره و کاربرد آن‌ها در قسمت‌های بعدی توضیح داده خواهد شد.