Active Directory

Subsystems:

یکی از قابلیتهای Win2k امکان اجرای برنامه هایی می باشد که تحت سیستم عاملهای دیگر نوشته شده اند. برای آنکه یك برنامه بتواند با سیستم عامل ارتباط برقرار نماید باید تحت Application Programing Interface (API) های آن سیستم عامل نوشته شده باشد. ویندوز چندین API اضافی را برای بوجود آوردن امکان اجرای برنامه های مربوط به سیستم عاملهای دیگر در خود گنجانده است که به آنها Subsystem می گویند. بدین معنا که Subsystem ها درخواست ها را از برنامه ها دریافت نموده و به سیستم عامل یا OS منتقل می کنند.

برنامه هایی که با استفاده از این Subsystem ها اجرا می گردند بهمراه خود این Sub System ها دارای محدودیت های زیر می باشند:

- دسترسی مستقیم به سخت افزار ندارند.
- دسترسی مستقیم به Driver ها ندارند.
- در آدرس های معلومی که در حافظه محدود می باشند باید اجرا شوند.
- در صورتیکه سیستم نیاز به حافظه داشته باشد، باید از روی Ram به روی Hard منتقل شده و از حافظه مجازی استفاده نمایند.
- نسبت به پردازشهای مربوط به Kernel، دارای اولویت کمتری می باشند.

Directory :

شامل اطلاعات مربوط به منابع شبکه می باشد. یافتن و کنترل منابع را ساده می نماید.

Directory Service :

یك سرویس شبکه است که تمام منابع موجود بر روی یك شبکه را تشخیص داده و آنها را بر اختیار برنامه ها و کاربران می گذارد.

سازگاری Active Directory (AD) :

ADمی تواند برای تبادل اطلاعات با هر برنامه یا Directory دیگري، از پروتکلهای LDAP یا HTTP استفاده کند. برای مثال ADمی تواند اطلاعات خود را با Novell Directory Service (NDS) هایی که از پروتکل LDAP با Version 2,3 استفاده می نمایند به اشتراك بگذارند.

فرمتهای نامگذاری استاندارد پشتیبانی شده در AD :

RFC 822 (همان E-Mail Address)

HTTP URL (آدرس های مورد استفاده در اینترنت)

UNC (مانند: \\Computer Name\Share Name)

LDAP URL (مانند: LDAP://servername.microsoft.com/CN=Firstname,OU=sys)

NTDS.DIT :

در این فایل اطلاعات اصلی AD ذخیره می گردد.

نکته :

هیچ کاربری نمی تواند بصورت local بر روی DC، login نماید. یعنی برای آنکه کاربری در پشت DC نشسته و بتواند بر روی آن login نماید باید بر روی AD (Domain) دارای یك account باشد. زیرا DC ها دارای Local Security

Database نمی باشند. در ضمن آن account باید دارای حق Log On Locally نیز باشد.

Object :

منابع ذخیره شده در directory از قبیل اطلاعات کاربر، چاپگرها، سرورها، گروه ها، کامپیوترها و security policy ها را object می گویند.

object یك نام مشخص برای مجموعه ای از صفات می باشد که یك منبع موجود در شبکه را توصیف می کند.

Classes :

در AD می توان object ها را نیز در class ها سازماندهی کرد. class ها یك دسته بندی منطقی از object ها می باشند.

نکته :

بعضی از object ها که container نیز به آنها گفته می شود، می توانند شامل چندین object دیگر باشند. برای مثال یك domain که می تواند شامل Userها، computerها و غیره باشد یك Container Object نام دارد.

AD Schema :

فهرستی از توضیحاتی است که انواع objectها و اطلاعاتی را که در رابطه با آن objectها می توان در AD ذخیره نمود، مشخص می نماید. بنابراین اگر بخواهیم attribute های جدیدی را به همراه object ها تعریف نمائیم باید در schema تغییرات لازم را انجام دهیم. (بصورت default مواردی که ویندوز به آنها نیاز دارد

در schema وجود دارند، اما در صورت نیاز نیز می توان در schema تغییرات ایجاد نموده و مواردی را به آن اضافه نمود. برای مثال برنامه هایی مانند Exchange Server و ISA Server در هنگام نصب object های مورد نیازشان را به schema می افزایند.)

دو مشخصه در Schema وجود دارد:

۱. Attributeها

۲. Classها

به این دو پارامتر Schema Object یا Meta Data می گویند.

attribute ها جدا از class ها تعریف می گردند. هر attribute فقط و فقط یکبار تعریف شده و می توان آنرا در چندین class مورد استفاده قرار داد.

برای مثال صفت description در خیلی از class ها مورد استفاده قرار می گیرد. ولی در schema فقط یکبار تعریف می شود. کلاس ها که Object Classes نیز نامیده می شوند object هایی را که در AD قابل ایجاد شدن می باشند را مشخص می نمایند. (مانند: account، group، printer و...)

Domain :

اصلی ترین ساختار منطقی موجود در AD می باشد که می تواند میلیونها object را ذخیره کند. AD می تواند از یك یا چند domain تشکیل گردد. هر domain بصورت تئوری تا ۱۰/۰۰۰/۰۰۰ و بصورت عملی تا ۱/۰۰۰/۰۰۰ object را می تواند در خود جای بدهد.

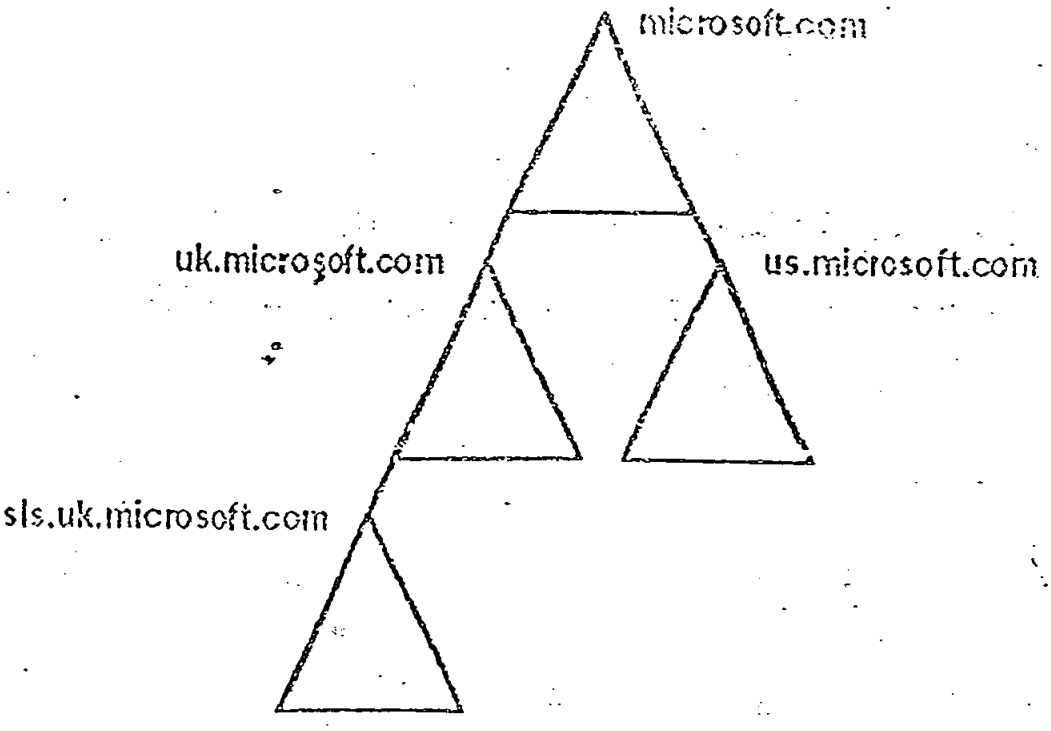
Organization Unit (OU) :

یك container است كه برای سازماندهی object ها در یك domain مورد استفاده قرار می گیرد. یك OU می تواند شامل object هایی مانند User، Group و Computer باشد. در ضمن یك OU را می توان در داخل OU دیگر قرار داد. (پیشنهاد می شود كه حداكثر تا پنج level این كار انجام گیرد.)

Tree :

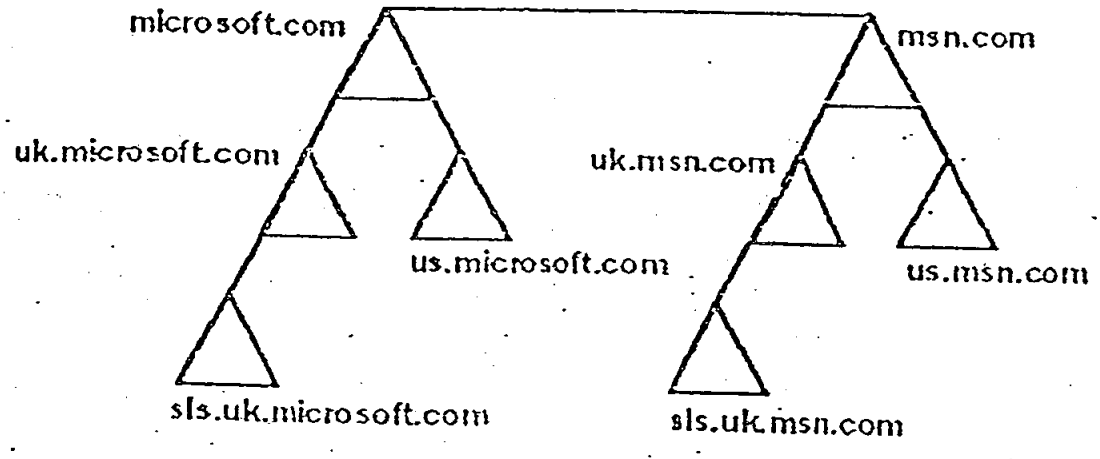
یك دسته بندی یا ساختار درخت واره ای (hierarchical) از یك یا چند Domain می باشد. دریك Tree تمام domain های موجود دارای یك نام DNSی وابسته به یكدیگر می باشند. (Contiguous Name Space)

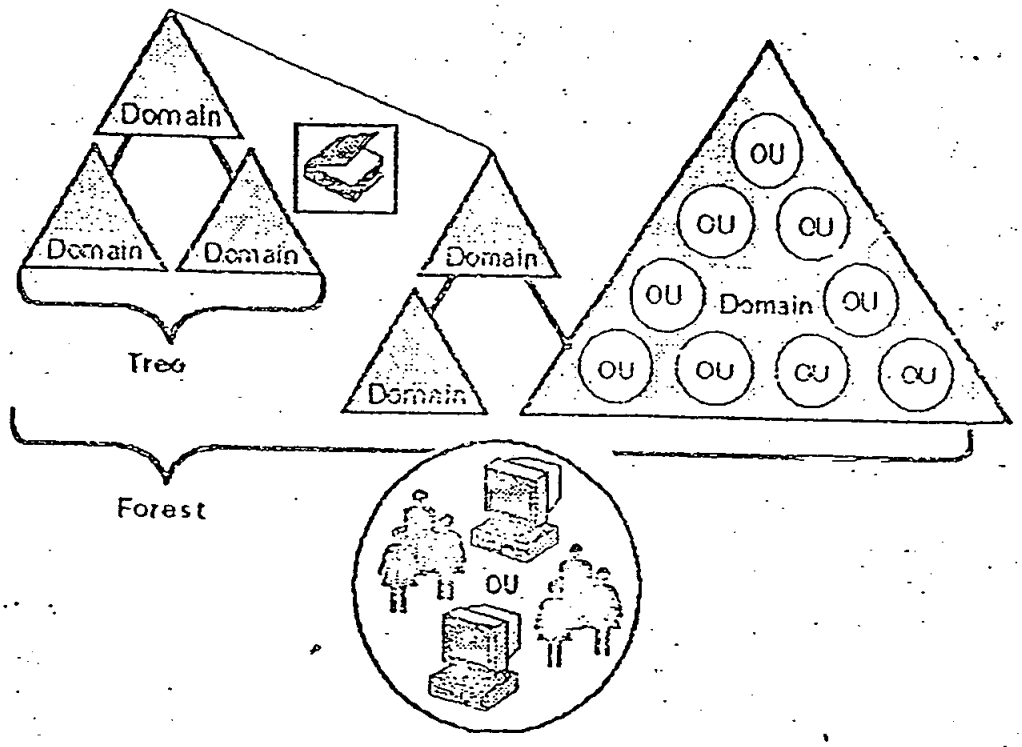
مانند: mft.com و sales.mft.com



Forest :

یك دسته بندی یا ساختار hierarchical است كه از یك یا چند tree كاملا جداگانه تشكیل می گردد.





Site :

ترکیبی از یك یا چند Subnet IP می باشد که در داخل آن کامپیوترها دارای یك ارتباط سریع و متعادل می باشند. یك domain می تواند به چندین site تقسیم گردد. یك site نیز می تواند چندین domain را شامل شود. زمانیکه یك domain ازلحاظ جغرافیایی حداقل در دو منطقه واقع شده باشد، بین مراکز مختلف این domain سرعت ارتباطی معمولا کمتر از سرعت موجود در هر کدام از مراکز است.

با استفاده از تعریف Site در AD و قراردادن حداقل یك DC مشخص در site های مختلف و جدا نمودن تمام کامپیوتر ها با استفاده از subnet های IP ، client های موجود در هر site را موظف می کنیم تا برای login نمودن ترجیحاً از DC موجود در site خود استفاده نمایند. اگر چنین کاری انجام نگیرد، چون یك client در یك domain می تواند بر روی تمام DCهای موجود در domain خود login نماید با مشکل روبرو خواهیم شد. چراکه بعضی از client ها درخواست login خود را به DC های موجود در مکانهای دیگر ارسال می نمایند و چون سرعت ارتباطی کندتر می باشد، login ها مدت زمان بیشتری را نیاز خواهند داشت.

خصوصیات DC:

۱. هر DC نسخه کاملی از اطلاعات AD، domain خود را ذخیره می نماید.
۲. DCها هر گونه تغییر انجام شده در AD را با یکدیگر Replicate می نمایند.
۳. DCها تغیرات مهمی از قبیل Disable شدن یك Account را بی درنگ Replicate می نمایند.
٤. در AD، Replication بصورت multimaster می باشد. بدین معنا که هر کدام از DCها می توانند در AD تغییر ایجاد نموده و آن تغییر را به سایر DCها Replicate نمایند.

Global Catalog (GC):

مرکز ذخیره اطلاعات مربوط به Objectهای موجود در یك Tree یا Forest می باشد.

GC بصورت اتوماتیك بر روی اولین DC موجود در Forest ایجاد می گردد که آن DC را Global Catalog Server نیز می نامند.
این سرور نسخه کاملی از Attribute های تمام Object های موجود در Domain خود را بعلاوه قسمتی از صفتهای تمام Object های Domain های دیگر موجود در Forest خود ذخیره می نماید.

وظایف GC :

۱. زمانیکه یك User بر روی شبکه Login می کند، GC اطلاعات مربوط به عضویت آن User در Universal Groups را در اختیار سرویس Logon قرار می دهد. اگر در هنگام فرایند Login یك User، GC وجود نداشته باشد آن User فقط می تواند بر روی کامپیوتر محلی بصورت locally، login نماید.

نکته مهم:
اگر GC در شبکه موجود نباشد، فقط اعضای گروه Domain Admins و افرادی که login آنها بر روی کامپیوتر مربوطه cache گردیده است می توانند در domain، logon نمایند.

۲. کمك می کند تا اطلاعات لازم مربوط به هر کدام از domain های موجود در forest را بدست آوریم.

تعداد GC Server های مورد نیاز : بهتر است که در هر سایت حداقل یکی از این سرورها موجود باشد تا Clientها در هنگام جستجو و Login نمودن سریعتر بتوانند با GC ارتباط برقرار کرده و نیازهای خود را برآورده سازند.

Replication :

اطلاعات ذخیره شده در Directory به سه قسمت تقسیم می گردند که به هر کدام Directory Partition می گویند:

۱. Schema Information :

شامل اطلاعات مربوط به Object هایی (بهمراه attribute های مربوط به آنها) است که می توانند در Directory ایجاد شوند. این اطلاعات در تمام Domain های موجود در Tree یا Forest مشترک می باشد.

۲. Configuration Information :

این قسمت شامل توضیحات مربوط به ساختار منطقی شبکه از قبیل ساختار Domain یا Topology مربوط به Replication می باشد. این اطلاعات بین تمام Domain های موجود در یک Tree یا Forest یکسان است.

۳. Domain Data :

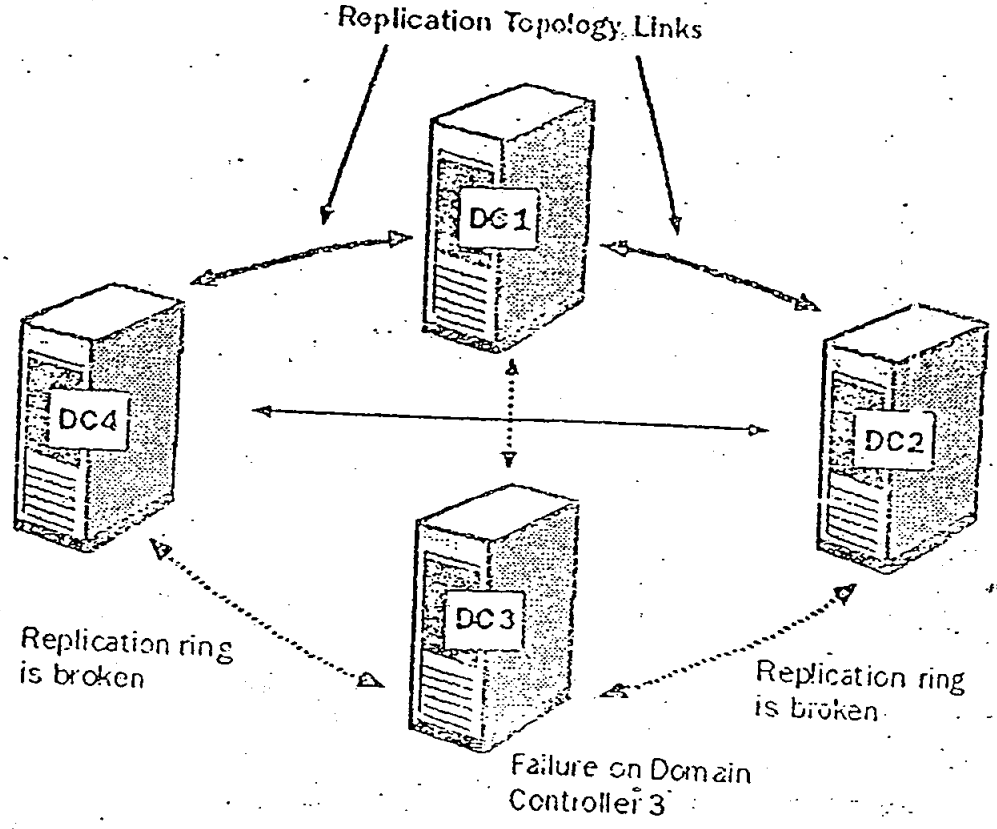
این قسمت تمام Object های موجود در یک Domain را شرح می دهد. این اطلاعات مختص Domain می باشد و به Domain های دیگر منتقل نمی گردد. اما قسمتی از آنها بخاطر توضیحات داده شده در GC ذخیره می گردد.

چگونگی کارکرد Replication :

در داخل یک سایت Replication بین DCها دارای Topology منطقی Ring می باشد. ولی برای اینکه در صورت قطع شدن یک DC از شبکه در این

Topology مشکلی رخ ندهد هر DC دو DC دیگر را جهت Replication انتخاب می کند تا در صورت برقرار نشدن ارتباط با یکی از DCها به سراغ DC دوم برود.

در شکل زیر DC3 دچار اشکال گردیده است، ولی replication ادامه دارد:



Knowledge Consistency Checker (KCC) :

وظیفه بوجود آوردن و کنترل Replication بین DCها در داخل یک سایت را بر عهده دارد. (بصورت پیش فرض هر ۵ دقیقه یکبار Replication رخ می دهد)

Replication بین سایت ها :

برای اینکه بین DCهای مختلف در سایت های مختلف Replication رخ دهد، باید ما تنظیمات لازم را انجام دهیم و بصورت دلخواه زمانهای Replication را انتخاب نماییم.

Trust Relationship:

ارتباطی است بین دو Domain که سبب می شود تا Domain اعتماد کننده Login های انجام شده در Domain دیگر را (که به آن اعتماد نموده است) بپذیرد.

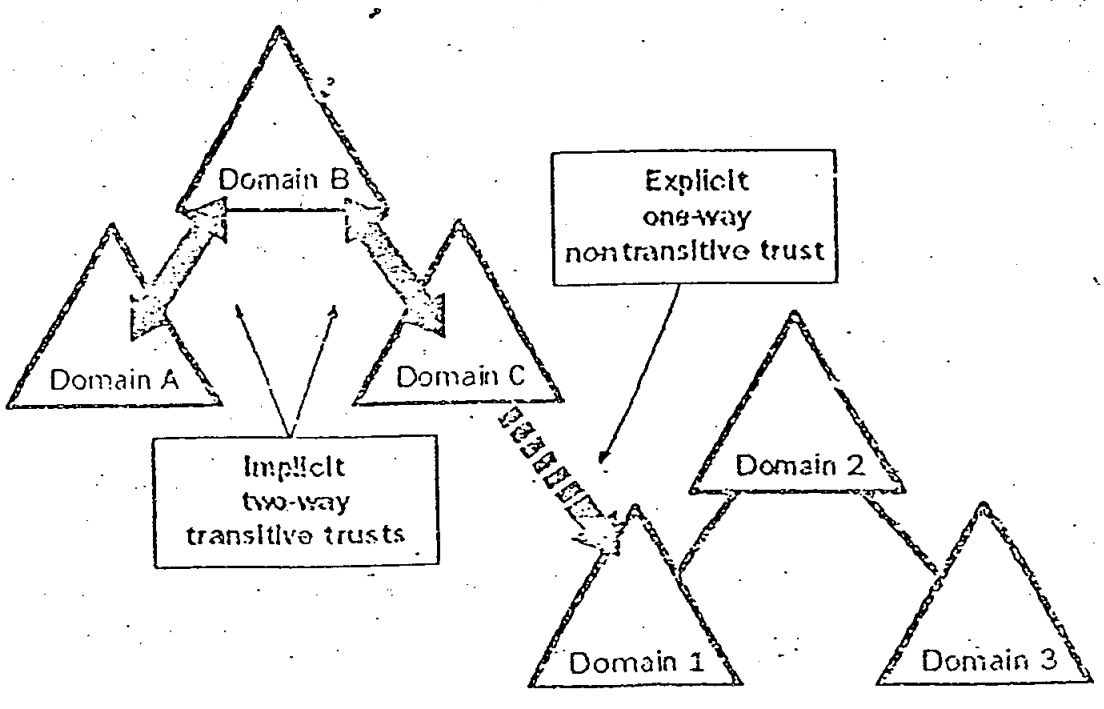
در Win2k دو نوع Trust وجود دارد :

1. Implicit two – way transitive trust
2. Expilicit one – way nontransitive trust

نوع اول بصورت اتوماتیک بین Parent و Child در یک Tree و بین دو Parent در یک Forest بوجود می آید.

نوع دوم بین Domain هایی که عضو Tree یا Forest یکسانی نمی باشند بوجود می آید و در ضمن تنها حالتی است که می توان در شرایط زیر Trust ایجاد کرد :

- بین یک Domain 2000 و یک Domain NT
- بین Domain یک Forest با Domain یک Forest دیگر. (هر دو ۲۰۰۰)
- بین یک Domain 2000 و شبکه ای که از Kerberos V5 مربوط به MIT استفاده می نماید.



DNS: (رجوع شود به infrastructure)

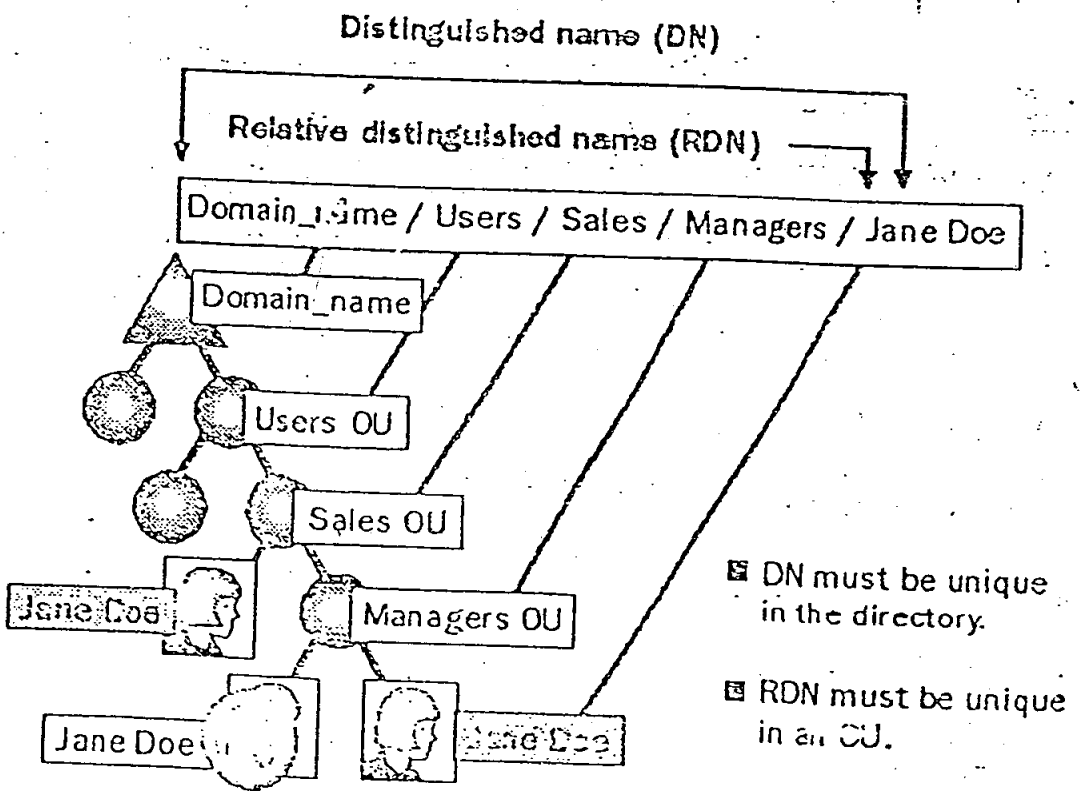
Distinguished Name (DN) :

هر Object در AD دارای یک DN می باشد که منحصرا یک Object را مشخص نموده و اطلاعات لازم جهت دسترسی به آن Object را در بردارد. بنابراین در AD هیچگاه نمی توان دو Object با DN یکسان داشت.

Relative DN (RDN):

RDN مربوط به یک Object قسمتی از نام آن می باشد که بصورت یک Attribute برای آن Object می باشد. برای مثال نام و نام خانوادگی یک User می تواند RDN آن باشد.

RDN باید در یک OU منحصربفرد باشد. زیرا در غیر اینصورت دو Object بوجود می آید که دارای DN یکسان می باشند.



Globally Unique Identifier (GUID) :

یک عدد ۱۲۸ بیتی است که منحصر بفرد می باشد. زمانیکه Object ها ایجاد می گردند GUID به آنها اختصاص داده می شود. (هر Object دارای یک GUID منحصر بفرد است) این عدد در تمام Domain ها منحصر بفرد است. بنابراین ما می توانیم بدون اینکه نگران Conflict بینGUIDها باشیم، یک Object را از یک Domain به Domain دیگر منتقل نماییم.

User Principal Name (UPN) :

این اسم که User Friendly می باشد شامل User Name و Domain مربوطه بصورت فرمتی که در آدرس های e-mail استفاده می گردد، می باشد.

مانند: Ali@Mft.Com

AD Administrative Tools:

برای نصب کنسولهای دیگر AD بعد از نصب AD، در منو Run دستور adminpak.msi را تایپ می کنیم.

Console ها:

Active Directory Domains and Trusts

با این کنسول می توان کارهای زیر را انجام داد :

- برقراری ارتباط با Domain های دیگر توسط ایجاد Trustهای Explicite
- تغییر حالت Win2k Domain از حالت Mixed به حالت Native
- حذف و اضافه پسوندهای UPN مخصوص User Name ها
- انتقال وظیفه Domani Naming Oprations Master

- ارائه اطلاعات درباره مدیریت Domain

✓ Active Directory Sites and Services

با این کنسول می توان تمام عملیات مربوط به تعریف و تنظیم سایتهای AD (قسمتهای فیزیکی) را انجام داد. AD با استفاده از تنظیمات انجام شده در این کنسول replication بین سایتها را انجام می دهد.

✓ Active Directory Users and Computers

با این کنسول می توان user account ها، computer accountها، گروهها و OU ها را ایجاد، تغییر و یا حذف نمود. در ضمن به ما امکان می دهد تا domain را با تعریف group policy ها کنترل نماییم.

تعریف Support Tools :

یکسری از فایل های مورد استفاده در AD که در جدول ۲-۳ صفحه۶۵ کتاب توضیح داده شده اند توسط Win2k Support Tools در دسترس قرار می گیرند. برای نصب آنها باید فایل setup.exe واقع در شاخه Support\Tools موجود در CD مربوط به Win2k Server را اجرا نمائیم. برای نصب این قسمت حداکثر به 18.2 Mb فضا نیاز داریم.

فایل movetree.exe :

توسط این فایل می توان Object هایی از قبیل OU و User ها را در یک Forest بین domain ها منتقل نمود.

پیاده سازی AD

دلایلی که سبب می شوند تا نیاز به ایجاد یک domain جدید داشته باشیم :

- تقسیم مدیریت شبکه
- کنترل Replication (کاهش ترافیک)
- سازمانهایی که نیاز به سیاستهای مختلفی جهت تعیین Password دارند.
- تعداد بسیار زیاد Object ها
- نام Domain های مختلف در Internet
- نیازهای جهانی: برای مثال ممکن است در هر قسمت از جهان نیاز به دارا بودن یک Domain باشیم. اگر بخواهیم تمام پایگاهها را تحت یک Domain کنترل نماییم بسیار مشکل خواهد بود.
- نیازهای سیاست داخلی

طراحی DNS :

برای ایجاد یک Domain باید یک Namespace برای آن در نظر بگیریم و سیستم DNS را بر اساس آن پیاده نماییم.

پیاده سازی DNS برای هر Domain دارای دو حالت می باشد:

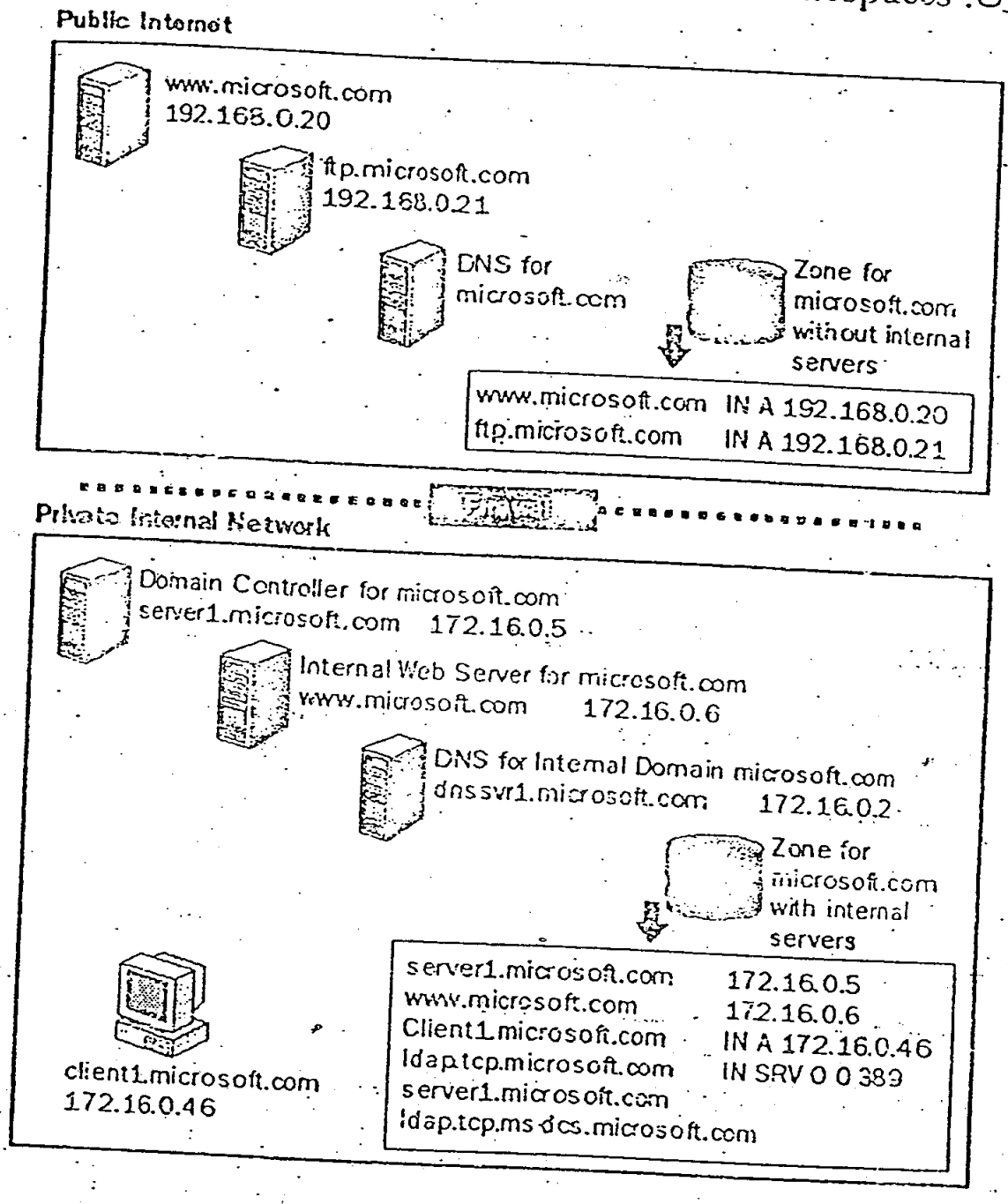
۱ – اسم Domain داخلی با اسم Domain خارجی یکسان باشد.

۲ – اسم Domain داخلی با اسم Domain خارجی یکسان نباشد.

نکته :

بین DNS داخلی و خارجی Firewall قرار دارد.

حالت اول: Same Internal and External Namespaces



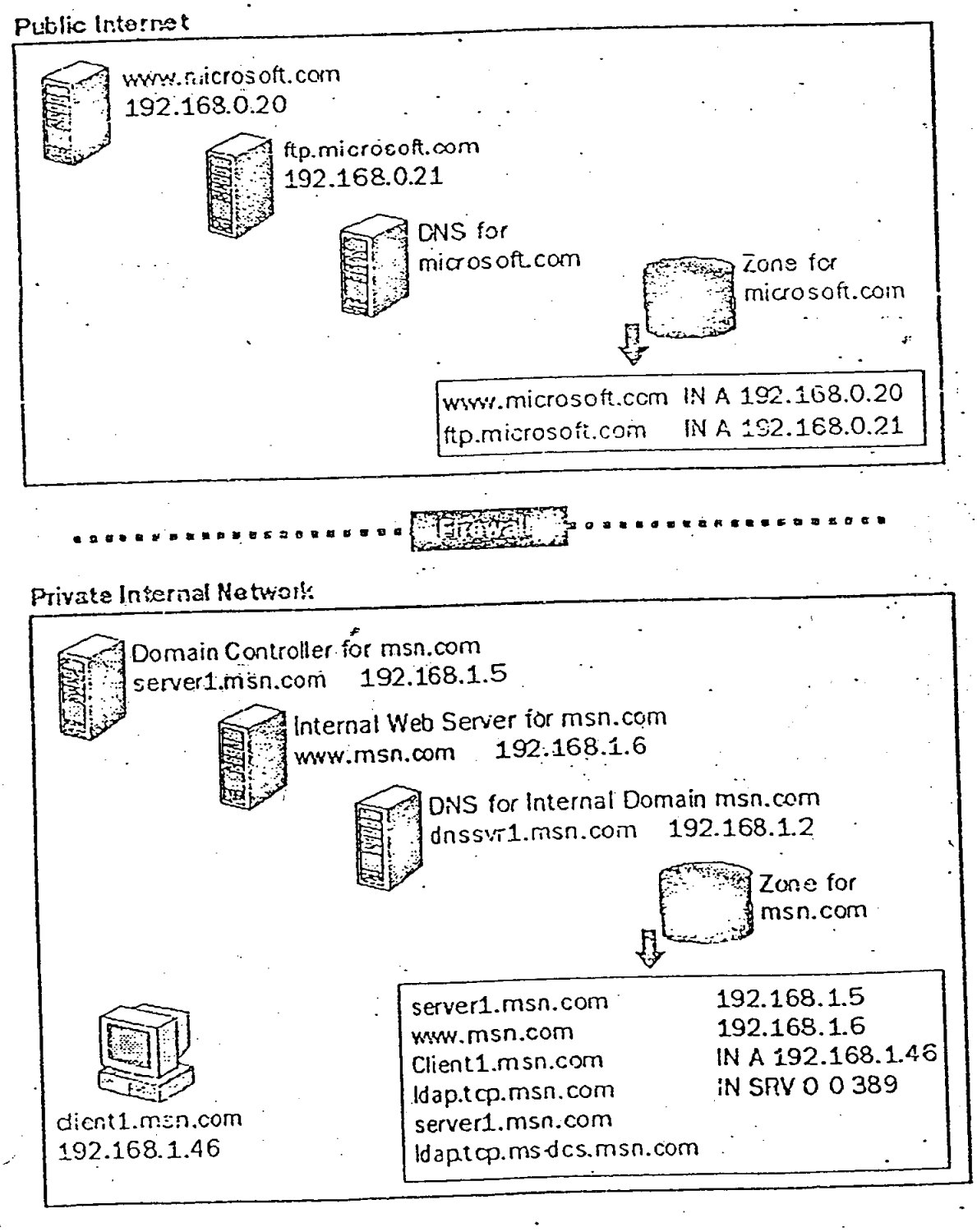
مزایای حالت اول :

- آدرسهای Email کاربران چه در داخل Domain و چه در خارج از Domain یکسان می باشد.
- فقط نیاز به ثبت یک Domain وجود دارد (در اینترنت)

معایب حالت اول :

- تمام عملیات مربوط به DNS داخلی را باید عینا دوباره بر روی DNS خارجی انجام دهیم.
- کنترل DNS ها بدلیل اینکه هر دو دارای یک Namespace می باشند، سخت تر و پیچیده تر می باشد.

حالت دوم: Separate Internal and External Namespaces



مزایای حالت دوم :

- از آنجا که Domain Name داخلی با خارجی متفاوت است کنترل DNS ها ساده تر می باشد.

معایب حالت دوم :

- دو Domain Name را باید در Internet به ثبت رساند.
- آدرس Email کاربران در داخل Domain با آدرس آنها در Internet متفاوت خواهد بود اگر چه می توان با ایجاد تغییر در UPN این مطلب را بر طرف نمود.

Operations Master Roles :

همانطور که قبلا توضیح داده شده با اینکه Win2k Domain بصورت Multimaseter می باشد با این حال بعضی از عملیات در Domain بصورت Singlemaster می باشد.

۱. Schema Master :

این DC تمام update ها و تغییرات ایجاد شده در schema را کنترل می نماید. در هر Forest یک عدد Schema Master می تواند وجود داشته باشد. برای آنکه تغییری در Schema ایجاد نماییم باید بتوانیم به Schema Master دسترسی پیدا کنیم. با استفاده از کنسول Schema می توان اینکار را انجام داد البته به شرطی که عضو گروه Schema Admins باشیم.

۲. Domain Naming Master :

اضافه یا حذف نمودن Domainها در یک Forest را کنترل می نماید. فقط یک Domain Naming Master می تواند در Forest (در هر لحظه) وجود داشته باشد.

۳. Relative ID Master Role :

این DC زمانیکه یک user، group و یا computer object در domain ایجاد می گردد به آن یک Security ID منحصر بفرد اختصاص می دهد.

برای اینکه یک Object را بین domain ها منتقل کنیم (بااستفاده ازدستور movetree.exe) باید این عملیات را بر روی DCهایی که وظیفه Relative ID Master را بعهده دارند انجام دهیم. در هر domain در هر لحظه فقط می تواند یك RID Master وجود داشته باشد.

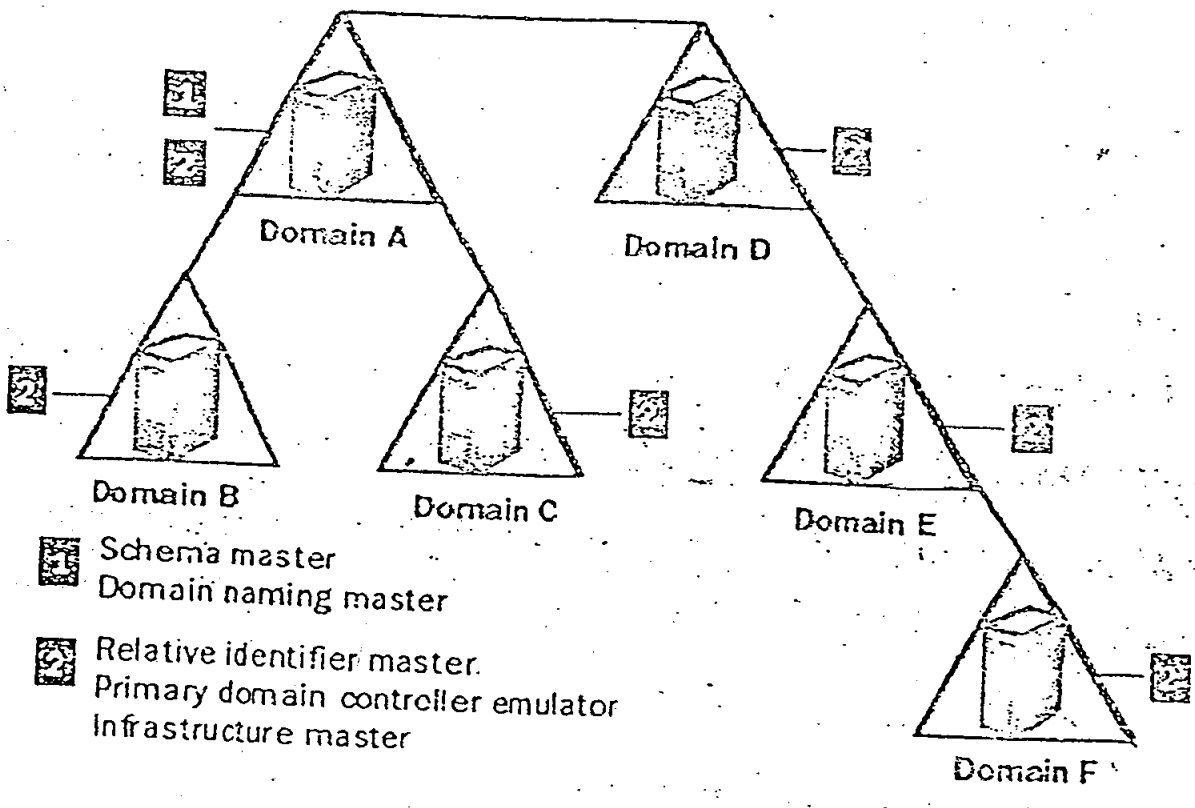
۴. PDC Emulator Role :

اگر domain دارای کامپیوترهایی با OS هایی غیر از Win2k باشد یا در آن BDC وجود داشته باشد، PDC Emulator بعنوان یك PDCعمل کرده و تغییرات Password مربوط به client ها و Replication با BDCها را برعهده خواهد گرفت. حتی اگر تمام سیستم ها نیزبه Win2k، upgrade شوند و domain Win2k در حالت Native Mode باشد PDC Emulator همچنان یک وظیفه برعهده خواهد داشت. بدین ترتیب که password های تغییر یافته را از DCهای دیگر دریافت کرده و Replication لازم را انجام می دهد. می دانیم که اگر password تغییر یابد تا این تغییر به DCهای دیگر منتقل گردد مدت زمانی طول خواهد کشید ولی PDC Emulator اولین DC خواهد بود که این تغییر را دریافت

می نماید. بنابر این اگر عملیات Logon Authentication بر روی یک DC بعلت password اشتباه انجام نگیرد درخواست Logon قبل از اینکه رد گردد به PDC Emulator منتقل می شود تا او نیز بررسی لازم را انجام دهد و ... .

۵. Infrastructure Master Role :

این DC وظیفه update نمودن ربط و بسط های ارتباطات مربوط به عضویت user در گروها را در زمانی که عضویتها تغییر یافته یا تغییر نام ایجاد می گردد بر عهده دارد.



اولین DCی که باعث بوجود آمدن یک Forest گردد تمام ۵ وظیفه را در ابتدا بر عهده خواهد داشت.

اولین DCی که یک Domain را در یک Forest که قبلا وجود داشته است بوجود آورد وظایف ۳، ٤ و ۵ را بعهده خواهد داشت.

توضیح داده شده را دوباره عینا تکرار می کنیم و برای انتقال Schema Master به کنسول Active Directory Schema وارد شده و عینا مراحل فوق را تکرار می کنیم.

حالت دوم

زمانی که Operation Master بصورت offline باشد در این حالت کامپیوتری که Operation Master بر روی آن قرار دارد در دسترس نمی باشد و برای اینکه Operation Master را به یک کامپیوتر دیگر اختصاص دهیم باید از دستور ntdsutil.exe استفاده نمائیم. (دستور roles را در ntdsutil اجرا کرده و Operation Master مورد نظر را seize کرده و به کامپیوتر (DC) مورد نظر اختصاص می دهیم) اما نکات زیر را حتما باید قبل از اینکار در نظر داشته باشیم:

- اینکار آخرین عملی خواهد بود که انجام می دهیم. یعنی حتی الامکان سعی می کنیم تا DCی را که offline شده است به حالت online بر گردانیم.
- اگر Role های Domain Naming , Schema Master و یا RID Master را seize نمودیم، DCی که این role را بر عهده داشته است را قبل از اینکه وارد شبکه کنیم باید حتما فرمت نموده و دوباره OS را بر روی آن نصب نماییم: ولی اگر بخواهیم می توانیم Infrastructure Master یا PDC Emulator را پس از بر طرف شدن مشکلشان به شبکه باز گردانده و دوباره Role مربوطه را به آنها برگردانیم (نیازی به فرمت شدن ندارند).

Site :

سایت به مجموعه ای از DCها گفته می شود که با سرعت کافی به یکدیگر متصل شده اند. برای اینکه ترافیک رد و بدل شده بین مکانهای مختلف فیزیکی موجود در

یک Domain را کنترل نماییم، هر کدام از آن مکانها را به عنوان یک سایت تعریف می کنیم. (با استفاده از مشخص نمودن یک رنج IP)
حداقل سرعت پیشنهادی بین سایت ها 512 Kbps می باشد.

ایجاد سایت :

توسط کنسول Active Directory Sites and Services تمام عملیات مربوط به سایتها و حتی تعیین GC ها را می توان انجام داد. پس از اینکه یک سایت ایجاد نمودیم، باید برای آن سایت یک Subnet و حداقل یک DC نیز تعریف کنیم.

Site Link :

برای اینکه دو یا چند سایت بتوانند با یکدیگر replication انجام دهند باید بین آنها حداقل یک Site Link وجود داشته باشد. هر Site Link می تواند یکی از پروتکلهای زیر را استفاده نماید:

- IP (RPC : Remote procedure call)
- SMTP

IP Replication :

این حالت از RPC جهت Replication استفاده می نماید و نیاز به CA (Certificate Authority) ندارد.

SMTP Replication :

این روش بر عکس حالت قبل فقط می تواند بین سایتهایی که عضو Domain های مختلفی می باشند، استفاده گردد و از آنجایی که SMTP بصورت غیر همزمان

(Asynchronous) عمل می کند، معمولا این روش از schedule هایی که در Site Link تعریف شده است پیروی نمی کند. درضمن در این روش نیاز به یک Enterprise CA داشته و تمام DCهایی که از این روش استفاده می کنند باید بر رویشان SMTP نصب گردد.

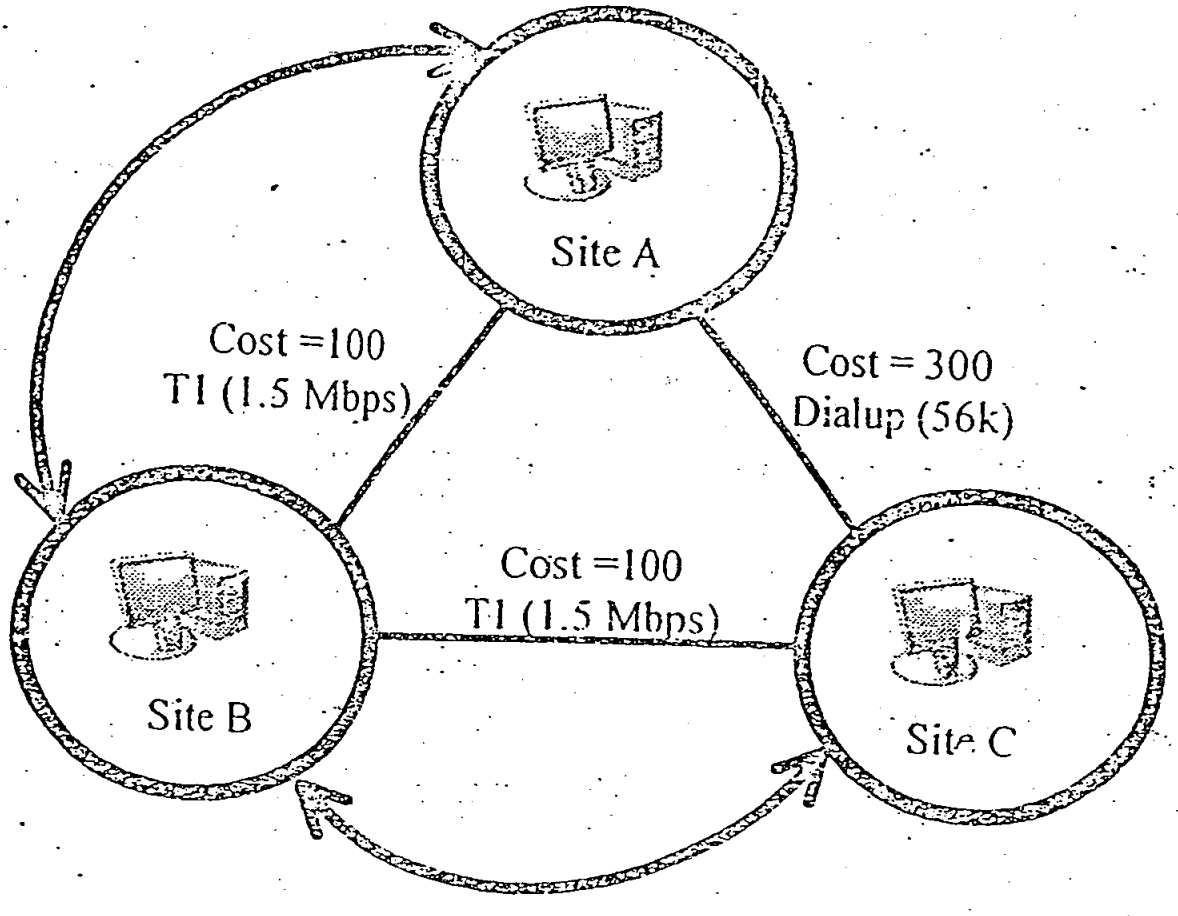
Site Licensing :

یک administrator می تواند license های خریداری شده برای Microsoft Back Office و نحوه استفاده از آنها را از طریق کنسول Licensing مشاهده نماید. ولی در هر سایت یکی از DCها را باید وظیفه جمع آوری اطلاعات مربوطه را بر عهده داشته باشد. اولین DCی که به یک سایت منتقل گشته یا اضافه می گردد بصورت پیش فرض این وظیفه را برعهده می گیرد و در صورت نیاز می توانیم آنرا به یک کامپیوتر دیگر (نیاز به یک DC نیست) منتقل نمائیم.

تنظیمات Site Link

Site Link Cost :

با استفاده از این پارامتر وضعیت یک Site Link را می توان از لحاظ ترافیک و سرعت مشخص نمود. بدین ترتیب که اگر بین دو سایت چندین مسیر جهت replication وجود داشته باشد می توان با تنظیم این مقدار بر روی Site Link های موجود در بین آن دو سایت مسیری را که ترجیح می دهیم تا repliation از طریق آن صورت گیرد مشخص نمود.



در شکل فوق Replication بین Site A و Site C از طریق مسیر نشان داده شده انجام می گیرد.

مگر اینکه یکی از خطوط T1 قطع شده باشد.

Replication Frequency :

با تنظیم این پارامتر می توان مشخص نمود که هر چند وقت یکبار بین سایتها Replication رخ دهد. (حداکثر 10080 دقیقه و حداقل 15 دقیقه)

Replication Availability :

با استفاده از دگمه Change Schedule در Properties یک Site Link می توان زمانهایی که در ۷ روز هفته در طول مدت ۲۴ساعت شبانه روز امکان

replication می تواند وجود داشته باشد را مشخص نماییم. برای مثال اگر بین ساعتهای بخصوصی ترافیک موجود در بین سایتها زیاد باشد بهتر است که در آن ساعتها امکان replication را از بین ببریم تا سرعت بین دو سایت کاهش پیدا نکند.

نکته :

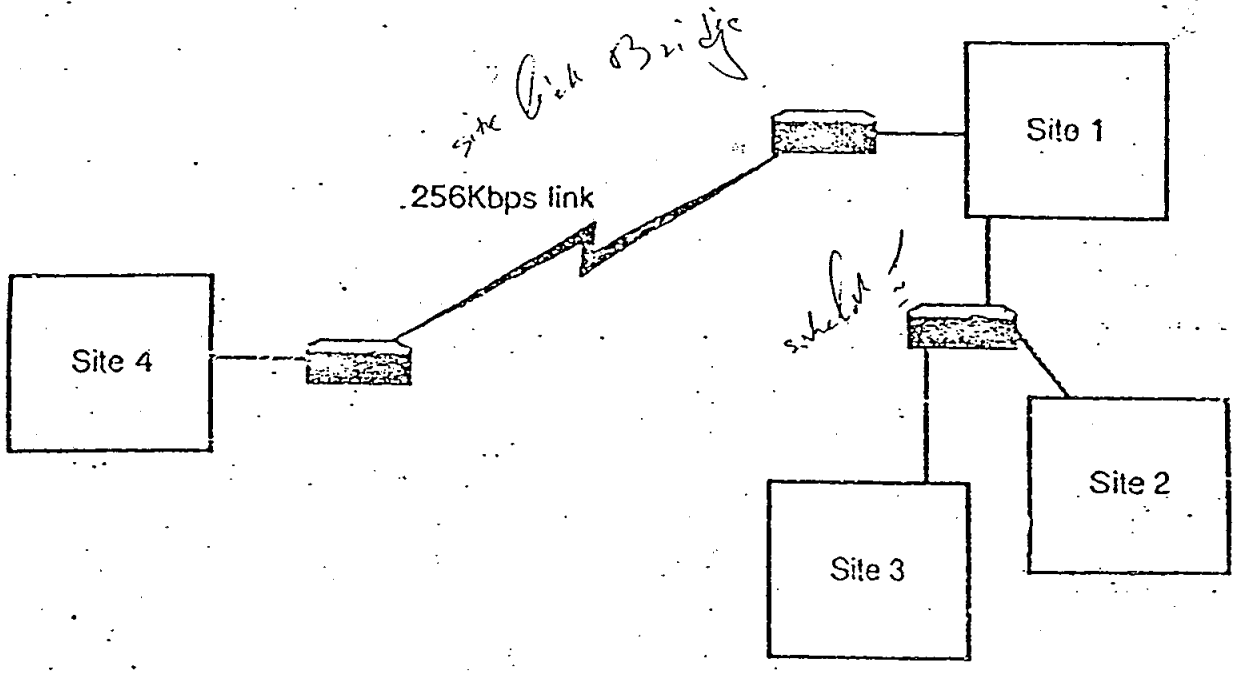
- برای Site Link هایی که در آنها از SMTP برای replication استفاده می نماییم بهتر است که Replication Availability تنظیم نکنیم. زیرا از آنجا که SMTP، Asynchronous می باشد، معمولا تمام Schedule ها را ignore می کند (نادیده می گیرد).
- اگر Ignore Schedules را در properties مربوط به Inter-Site Transport فعال کرده باشیم، دیگر schedule (زمانبندی) انجام شده در نظر گرفته نخواهد شد.

Site Link Bridges :

زمانیکه بیش از دو سایت جهت replication بهم مرتبط شده باشند و از transport یکسانی (SMTP یا IP) استفاده نمایند، بصورت پیش فرض با توجه به cost تنظیم شده تمام Site Link ها bridge می شوند و این bridge بصورت transitive می باشد.

در شکل قبل هر گاه سایت A با B replication انجام دهد، Site B نیز همزمان با سایت C می تواند replication نماید. ولی در شبکه هایی که ارتباط بین سایت های مختلف، کامل نمی باشد یا به عبارتی fully routed نمی باشد، باید خودمان بصورت manually یک Site Link Bridge ایجاد نموده و option مربوط به Bridge All Site Links را که در properties مربوط به Transport وجود

دارد deselect نماییم (انتخاب نکنیم). برای مثال در شکل زیر option توضیح داده شده باید deselect شده و Site Link Bridge بصورت manually ایجاد شود.



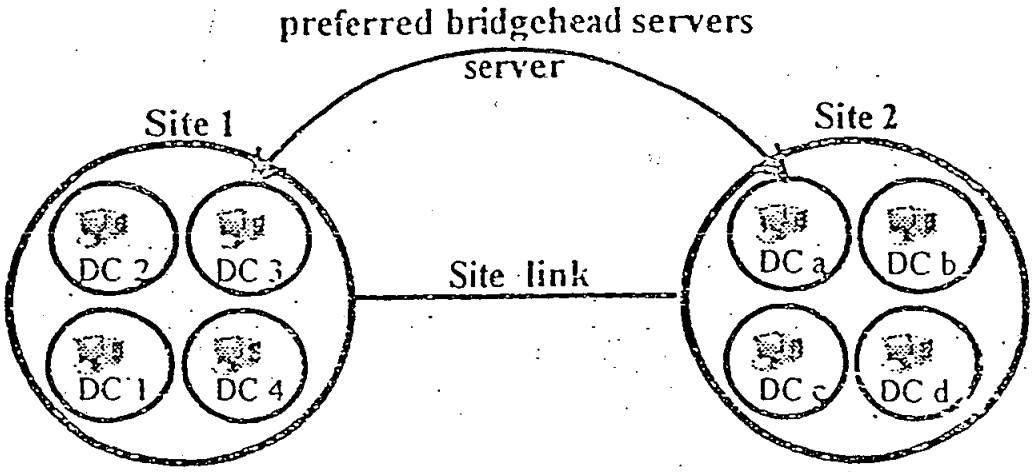
Manually Configuring Connections

AD بصورت اتوماتیک در حالت عادی بین DCهای مختلف مربوط به سایتها، connection بوجود آورده و delete می نماید و بهتر است در این روش تغییری بوجود نیاوریم. ولی در صورت نیاز می توان بین دوDC یک connection بوجود آورده و replication اجباری بین آن دوDC انجام دهیم.

Designating a Preferred Bridgehead Server

در حالت عادی replication بین دو سایت توسط هر کدام از DCها می تواند انجام گیرد، ولی در صورت نیاز می توان یکی از DCهای هر سایت را که دارای پهنای باند بیشتری (ترافیک کمتری) جهت replication می باشد، انتخاب کرده و آنرا

بعنوان یکDC در سایت که ترجیح می دهیم replication با سایتهای دیگر را او انجام دهد معرفی نمائیم.



در شکل فوق DC3 در سایت۱ و DC a در سایت۲ بدین صورت تنظیم گردیده اند.

نکته :

در هر سایت به هر تعداد که بخواهیم می توانیم Preferred Bridgehead Server تنظیم نماییم ولی در هر لحظه فقط یکی از آنها می تواند فعال باشد (DCی که اول انتخاب شده است). اگر سرور فعال، fail شود، AD یک Preferred Bridgehead Server دیگر را انتخاب می نماید. ولی اگر server دیگری با چنین تنظیمی وجود نداشته باشد، AD یک DC دیگر را بصورت اتوماتیک بعنوان Preferred Bridgehead Server انتخاب می نماید.

User Accounts:

در هنگام نصب IIS دو account با نامهای IUSER_*computername* و IWAM_*computername* ایجاد می گردند. Account اول جهت برقراری

ارتباط anonymous با IIS و دسترسی به آن و account دوم برای ایجاد دسترسی anonymous مخصوص برنامه های اضافی IIS مورد استفاده قرار می گیرد.
کاربر TSInternetUSER نیز در هنگام نصب terminal services بصورت اتوماتیك ایجاد گشته و توسط این سرویس مورد استفاده قرار می گیرد.

نکته :

در یك شبکه که کاملا ۲۰۰۰ می باشد، بهتر است که جهت کاهش ترافیك NetBIOS over TCP/IP را disable نماییم. (بهترین روش برای انجام اینکار، استفاده از optionهای DHCP server می باشد.) ولی باید توجه داشته باشیم که در صورت انجام اینکار دیگر win2k (AD) نمی تواند تشخیص دهد که شما بوسیله چه کامپیوتری login می نمایید و در نتیجه نمی توان user ها را مجبور کرد که برای logon نمودن فقط از کامپیوترهای بخصوصی (این مطلب را می توان در properties یك account تنظیم نمود) استفاده نمایند.

User Profiles :

یک profile شامل مجموعه ای از شاخه ها و اطلاعاتی است که تنظیمات برنامه ها، desktop و اطلاعات شخصی یك کاربر را ذخیره می نماید.
زمانیکه یک کاربر برای اولین بار بر روی یک کامپیوتر login می نماید، برای او یک Local User Profile ایجاد گشته و تنظیماتی که آن شخص انجام می دهد در هنگام logoff نمودن او در آنجا ذخیره می گردند و بار دیگری که کاربر دوباره login نمود، همان تنظیمات اعمال خواهند گردید. ولی اگر کاربر بر روی کامپیوتر دیگری login نماید دیگر آن تنظیمات اعمال نخواهند گردید. چراکه profile ها بصورت default محلی می باشند. برای اینکه بدون توجه به کامپیوتری که کاربر

جهت login نمودن استفاده می نماید، desktop و تنظیمات شخصی او همواره در تمام domain یکسان بوده و به همراه او منتقل گردد از Roaming User Profile استفاده می نماییم.

برای ایجاد نمودن چنین profileی کافیست که در قسمت profile مربوط به properties یک user مسیر محلی را که می خواهیم profile آن شخص بصورت متمرکز در آنجا ذخیره گردد، وارد نماییم. بدین ترتیب همواره profile آن شخص از آن محل خوانده شده و در آنجا ذخیره می گردد. (بهتر است که یک server را جهت ذخیره کردن profile ها در نظر بگیریم. بدین ترتیب که شاخه ای بر روی یک partition NTFS آن ایجاد نموده و آنرا share کرده و profile اشخاص را در آنجا ذخیره نماییم.) حال اگر بخواهیم profile آن کاربر بصورت اجباری (mandatory) درآید - بدان معنا که تغییراتی را که کاربر در profile ایجاد می نماید در هنگام logoff نمودن ذخیره نشوند - کافیست که در شاخه profile آن شخص فایلی با نام ntuser.dat را به ntuser.man تبدیل نماییم. با این عمل یک Mandatory User Profile ایجاد نموده ایم. (فایل ntuser.dat بصورت hidden می باشد)

گروه ها :

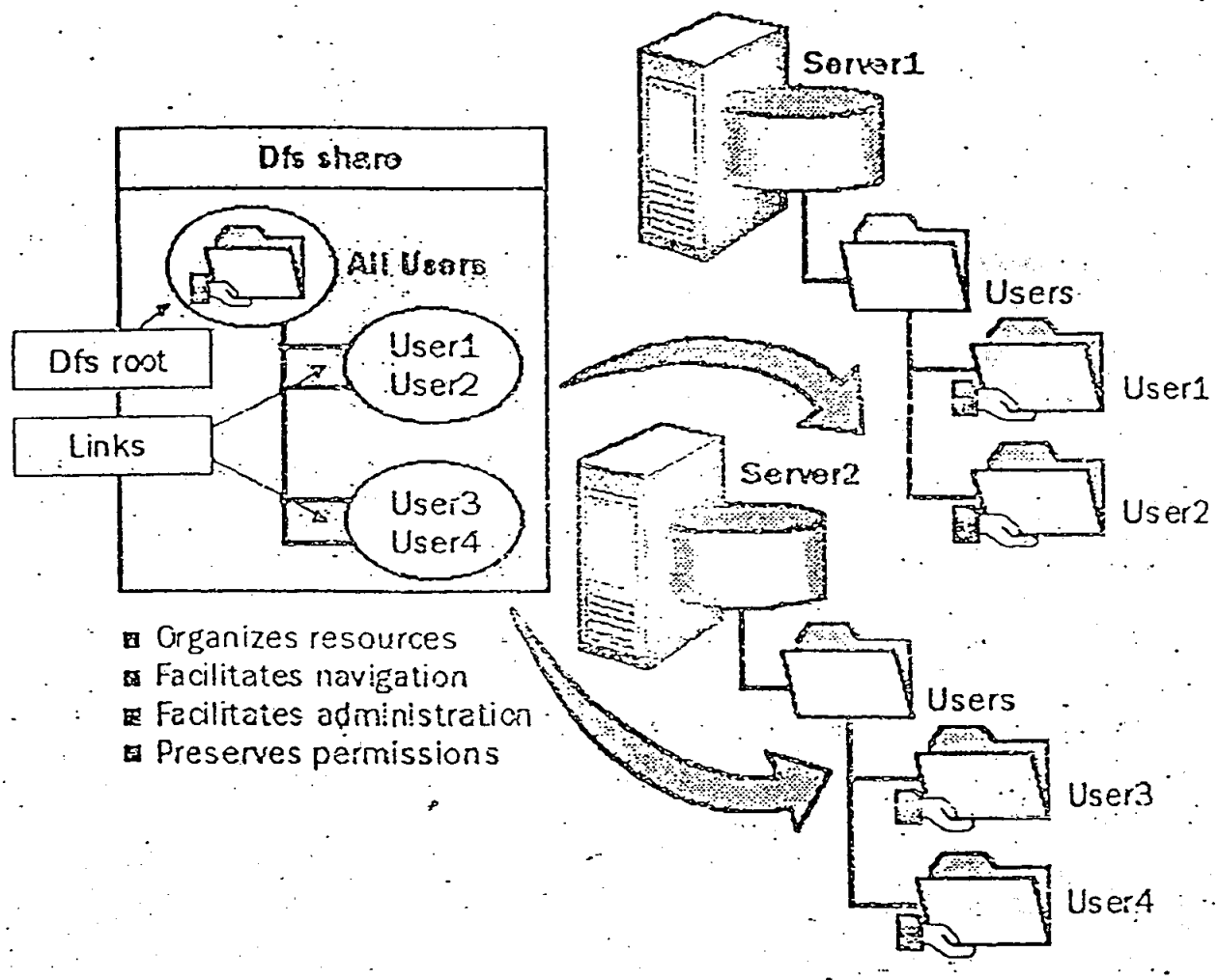
دو نوع گروه وجود دارد:

- Security
- Distribution

گروه اول جهت اختصاص permission و دسته بندی کاربران در شبکه ایجاد می گردد. (همان گروه عادی)

Distributed File System (Dfs):

با استفاده از این قابلیت می توان از تمام shareهای موجود در شبکه بر روی یک server یک link ایجاد نموده و دسترسی کاربران مختلف را به تمام share ها آسان نمود. بدین ترتیب فقط کافیست تا آنها به سرور Dfs متصل شده و از آنجا به تمام shareها دسترسی پیدا کنند.



دو نوع Dfs وجود دارد :

- Domain
- Standalone

در Dfs Domain - Share های موجود در شبکه می توانند محتویات خود را با یکدیگر replicate نمایند.

نکته :

فقط کامپیوتر هایی که دارای Dfs Client Software می باشند می توانند به منابع Dfs دسترسی پیدا کنند. مانند NT 4.0 به بعد و یا Win98. برای اینکه Win95 بتواند به Dfs متصل گردد باید نرم افزار مربوطه را download و برروی آن نصب نماییم.

حالتهای که استفاده از Dfs پیشنهاد می شود:

- کاربرانی که به شاخه های share شده دسترسی پیدا می کنند، دریک سایت یا چندین سایت قراردارند.
- بیشتر کاربران نیاز به دسترسی به چندین شاخه share شده دارند.
- بوسیله قراردادن چندین link مختلف به چندین server که همگی دارای محتویات یکسانی می باشند، بار وارد بر هر server متعادل می گردد.
- کاربران نیاز به دسترسی مستقیم به تمام شاخه های share شده دارند.
- سازمان شما دارای website های داخلی یا خارجی می باشد.

مراحل ایجاد یک Dfs :

- ایجاد یک Dfs root
- ایجاد یک Dfs link
- اضافه نمودن شاخه های share شده اضافی به یك Dfs link (اختیاری)
- تنظیم سیستم replication

در Dfs های Standalone، replication باید بصورت manually انجام شود، ولی در Dfsهای Domain، replication می تواند اتوماتیک نیز انجام گیرد.
در ضمن replication فقط زمانی اتوماتیک خواهد بود که اطلاعات ذخیره شده بر روی volumeهای NTFS قرار داشته باشد. بنابراین اطلاعاتی که در volume های FAT ذخیره شده اند باید بصورت manually، replicate گردند.

AD Permissions :

با استفاده از مجوزهای AD می توان دسترسی افراد مختلف را به object ها و attributeهای مربوط به objectها تعریف نمود - بااستفاده از Security tab - در صورت نیاز می توان با انتخاب Advance Features در منوی View به Security tab دسترسی پیدا کرد.

Publish کردن منابع در AD:

برای اینکه کاربران domain بتوانند با استفاده از جستجو در AD به منابع موجود و share شده کامپیوترهای مختلف دسترسی پیدا کنند، آن منابع باید در AD، publish شده باشند. پرینترهای share شده موجود بر روی Win2k ها بصورت اتوماتیک publish می شوند و در صورت نیاز می توان در properties پرینترها option، List in the Directory را غیر فعال نموده و از publish شدن پرینتر جلوگیری بعمل آورد.
پرینترهای NT بصورت اتوماتیک publish نمی شوند و برای publish کردن آنها دو راه وجود دارد:

- scriptی را که مایکروسافت در اختیار ما قرار داده است اجرا نموده و بهمراه وارد نمودن DN Printer آنرا در AD publish می کنیم.

cscript %systemroot%\system32\pubprn.vbs \\server03\5L
"LDAP://OU=Sales,DC=microsoft,DC=com"

باید توجه داشت که این script را فقط می توان برای publish کردن printerهای NT بکار برد.

- با استفاده از کنسول Active Directory Usera and Computers بر روی containerی که می خواهیم printer در آن publish شود، کلیک سمت راست نموده و پس از انتخاب گزینه new، printer را کلیک می کنیم و سپس نام UNC پرینتر share شده را وارد می کنیم.

انتقال object های AD :

برای انتقال object ها در داخل یک domain از کنسول Active Directory Users and Computers استفاده نموده و بر روی object مورد نظر کلیک سمت راست کرده و سپس Move را انتخاب می کنیم.

برای انتقال object ها بین domain ها از دستور movetree که پس از نصب Support Tools اضافه می گردد، استفاده می نماییم.

زمانیکه userها و گروها از یک domain به domain دیگر منتقل می گردند یک SID جدید به آنها اختصاص داده می شود. برای اینکه تمام جزییات آن user یا گروه (مانند permissionهایی که قبلا داشته است) همچنان برای او باقی بمانند Win2k در حالت native، قابلیتی با نام SID history را support می نماید. بدین ترتیب هر گاه که userها و گروها از یک domain به domain دیگر منتقل گردند، SID قدیمی آنها در attributeی با نام SIDHistory در objectی که جدیدا برای آنها ایجاد گردیده است، ذخیره می گردد و بدین ترتیب هر گاه userی یا گروهی بخواهد به منبعی دسترسی پیدا کند Access Control List (ACL) بر اساس هر دو SID

(جدید و قدیم) ایجاد و تنظیم می گردد. بنابراین user یا گروه پس از move شدن permission های قبلی خود را از دست نمی دهد.

عملیاتی که می توان با MOVETREE انجام داد :

- یک object یا یک container غیر تهی را می توان به یک domain دیگر منتقل نمود (فقط داخل forest).
- گروهای global و domain locoal را می توان بدون اعضای آنها به domain دیگر منتقل نمود (فقط داخل forest).
- گروهای universal را به همراه اعضایشان می توان به domain های دیگر منتقل نمود (فقط داخل forest)

موارد مهمی که نمی توان با MOVETREE منتقل نمود:

- گروهای global و local که شامل اعضا می باشند.
- کامپیوتر objectهای موجود دریک domain.
- اطلاعات مربوط به objectها از قبیل group policy ها، user profile ها، logon script ها، اطلاعات شخصی کاربران، فایلهای encrypt شده و ... .
- systme object ها (objectهایی که مخصوص سیستم می باشند و بعنوان system only علامتگذاری شده اند.)
- object های مربوط به configuration یا schema.
- object های مربوط به special container ها مانند lost & found
- DCها یا هر object دیگری که مربوط به یک DC می باشند.
- هر objectی که قبلا با همان نام در domain مقصد وجود داشته باشد.

ممکن است MOVETREE بخاطر خطاهای زیر کار نکند:

- DC منبع نتواند RID مالک را transfer نماید.
- objectی که می خواهیم آنرا منتقل نماییم بخاط عملیاتی که در حال انجام بر روی آن می باشد، قفل شده باشد.
- تنظیمات domain مبدا یا مقصد مشکل داشته باشد.
- domain مقصد تشخیص داده باشد که objectی که قرار است از domain مبدا منتقل گردد، قبلا حذف شده است ولی DC مبداء هنوز حذف شدن آن object را بدلیل replicate نشدن تشخیص نداده باشد.
- در domain مقصد اشکالی رخ دهد. برای مثال هارد دیسک آن پر شده باشد.
- به دلیل replicate نشدن صحیح schema، domain مبداء و مقصد از لحاظ schema داری اختلاف باشند.

MOVETREE {/start | /startnocheck | /continue | /check} /s *SrcDSA* /d *DstDSA* /sdn *SrcDN* /ddn *DstDN*[/u [*Domain*\]*Username* /p *Password*] [/verbose] [{/? | /help}]

مثال:

```
MOVETREE /start /s Server1.Marketing.Reskit.Com
/d Server2.Sales.Reskit.com
/sdn OU=Promotions,DC=Marketing,DC=Reskit,DC=Com
/ddn OU=test,DC=Sales,DC=Reskit,DC=Com
```

نکته:

برای انتقال object کامپیوتر هایی که عضو یک domain گردیده اند از دستور NETDOM استفاده می نماییم.

netdom move /D:*domain* [/OU:*ou_path*] [/Ud:*User* /Pd:{*Password*|*}]
[/Uo:*User* /Po:{*Password*|*}][/Reboot:[*time_in_seconds*]]

Backup و Restore نمودن AD:

برای اینکه از تمام AD موجود بر روی یک DC، backup تهیه کنیم از option مربوط به Backup System State Data در برنامه Backup استفاده می کنیم.

اگر بر روی یک server، System State را backup بگیریم، کل registry، database تنظیمات +COM، فایلهای مخصوص boot و در صورتیکه server ما certificate server باشد، database مربوط به Certificate Services نیز backup گرفته می شود.

و اگر server ما یک DC باشد، علاوه بر مطالب فوق، AD و شاخه sysvol نیز backup گرفته می شوند.

نکته ۱:

System State را فقط می توان بصورت localy، backup کرد. یعنی اطلاعات System State را نمی توان بر روی یک کامپیوتر remote، backup گرفت.

اگر بخواهیم backup را بر روی یک دستگاه removeable media تهیه نماییم، باید به موارد زیر توجه کنیم :

- هنگامی که System State را می خواهیم backup بگیریم، دستگاهی که قرار است backup را روی آن تهیه کنیم باید حتما به همان دستگاه (کامپیوتر) متصل گردیده و روشن شده باشد.
- media ی مربوطه باید در HCL وجود داشته باشد.

- media در داخل دستگاه مربوطه قرار داده شده باشد. برای مثال: اگر از tape استفاده می نماییم، باید tape در داخل آن قرار داشته باشد.

نکته ۲:

پس از اینکه System State را backup کردیم، در هنگام restore نمودن نمی توان قسمتی از آن را restore نمود. فقط تمام backup را می توان restore نمود.

نکته ۳:

اگر در هنگام restore کردن System State آنرا در alternat location (محل دیگری) restore نماییم، فقط وفقط فایلهای registry، فایلهای شاخه SYSVOL و فایلهای boot کننده سیستم در آن محل restore می گردند.

انواع Restore :

Nonauthoritative Restore :

در این روش ابتدا پس از restart نمودن سیستم، کلید F8 را فشار داده و سیستم را در حالت Restore Mode مخصوص DC راه اندازی می نماییم. از آنجا که در اینحالت AD راه اندازی نمی گردد، نمی توان با account هایی که در domain تعریف شده اند login نمود و باید با کاربر administrator که در هنگام نصب AD بر روی کامپیوتر، password آنرا تعریف نموده ایم، بر روی سیستم logon نماییم. سپس System State، backup شده را restore نموده و بعد از آن سیستم را بصورت عادی restart می نماییم و در نتیجه DC در صورت وجود DCهای دیگر شروع به replication نموده و اطلاعات از دست رفته دوباره بازیابی می

شوند. در این حالت اگر در domain، DC دیگری وجود نداشته باشد، تمام تغییراتی که از زمان backup گیری به بعد ایجاد نموده ایم از بین خواهد رفت.

Authoritative Restore :

اگر بصورت اشتباهی یکی از objectهای موجود در AD را delete یا تغییر دهیم، برای بازگرداندن موارد حذف شده یا تغییر داده شده از روش Authoritative Restore استفاده می کنیم. بدین ترتیب که همانند روش اول عمل نموده System State را restore نموده و پس از آن با استفاده از برنامه ntdsutil، version مربوط به objectهای restore شده را افزایش می دهیم. در نتیجه پس از آنکه در حالت عادی restore نمودیم، بجای آنکه مطالب تغییر یافته یا حذف شده از روی DCهای دیگر دوباره بر روی کامپیوتر ما (DC) منتقل گردند، مواردیکه ما restore نموده ایم بعلت بیشتر بودن version، بر روی DCهای دیگر replicate خواهند شد.

اگر تغییرات اشتباهی که بر روی DC انجام داده ایم به DCهای دیگر replicate نشده باشد، نیازی به روش دوم نمی باشد و استفاده از روش اول کافی است.

مثال: برای restore نموده یك OU با نام security1 در microsoft.com بصورت زیر عمل می کنیم:

```
NTDSutil
authoritative restore
restore subtree
OU=Security1,DC=Microsoft,DC=COM
```

Group Policy :

با استفاده از آن می توان تنظیات مربوط به یک user یا کامپیوتر را مشخص کرده و محدود نمود.

از دو قسمت تشکیل شده است :

- Computer Configuration
- User Configuration

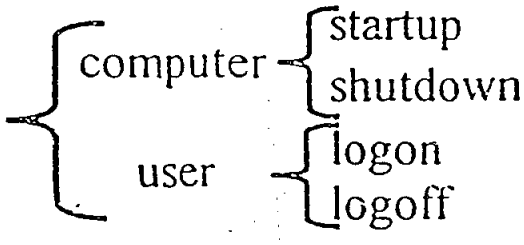
تنظیمات موجود در حالت اول بر روی کامپیوتر، بدون توجه به کاربری که بر روی آن login می نماید اعمال می گردد و زمانیکه OS راه اندازی می گردد، فعال می شود. تنظیمات موجود در حالت دوم به userی که logon می نماید در هنگام logon کردنش اعمال می شود.

هر کدام از قسمتهای فوق دارای سه قسمت مشترک می باشد:

۱. Software Settings
۲. Windows Settings
۳. Administrative Templates

Script :

برنامه ای است که توسط یك زبان برنامه نویسی مانند VB نوشته می شود و شامل دستور العملهایی می باشد. چهار نوع script می توان در policy تعریف نمود:



که ترتیب اعمال شدن آنها بصورت زیر می باشد:

1. startup
2. logon
3. logoff
4. shutdown

startup script ها بصورت hidden و synchronous اجرا می گردند و time out هر کدام از آنها ۱۰ دقیقه می باشد. یعنی اینکه به ترتیب پشت سر هم اجرا گردیده و تا یکی از آنها تکمیل نشده است دیگری اجرا نمی گردد و هر کدام از آنها حداکثر ۱۰ دقیقه فرصت دارند تا خاتمه یا بند.

logon script های موجود در system policy بصورت پیش فرض hidden و asynchronous اجرا می گردند.

یک GPO را می توان به موارد زیر با ترتیب نشان داده شده اعمال نمود:

۱. Local
۲. Site
۳. Domain
٤. OU

بنابراین اگر در GPO مربوط به یک OU تنظیمی انجام شده باشد که خلاف آن در domain GPO مربوط به آن OU تعریف شده باشد، تنظیم موجود در GPOی OU، override خواهد نمود.