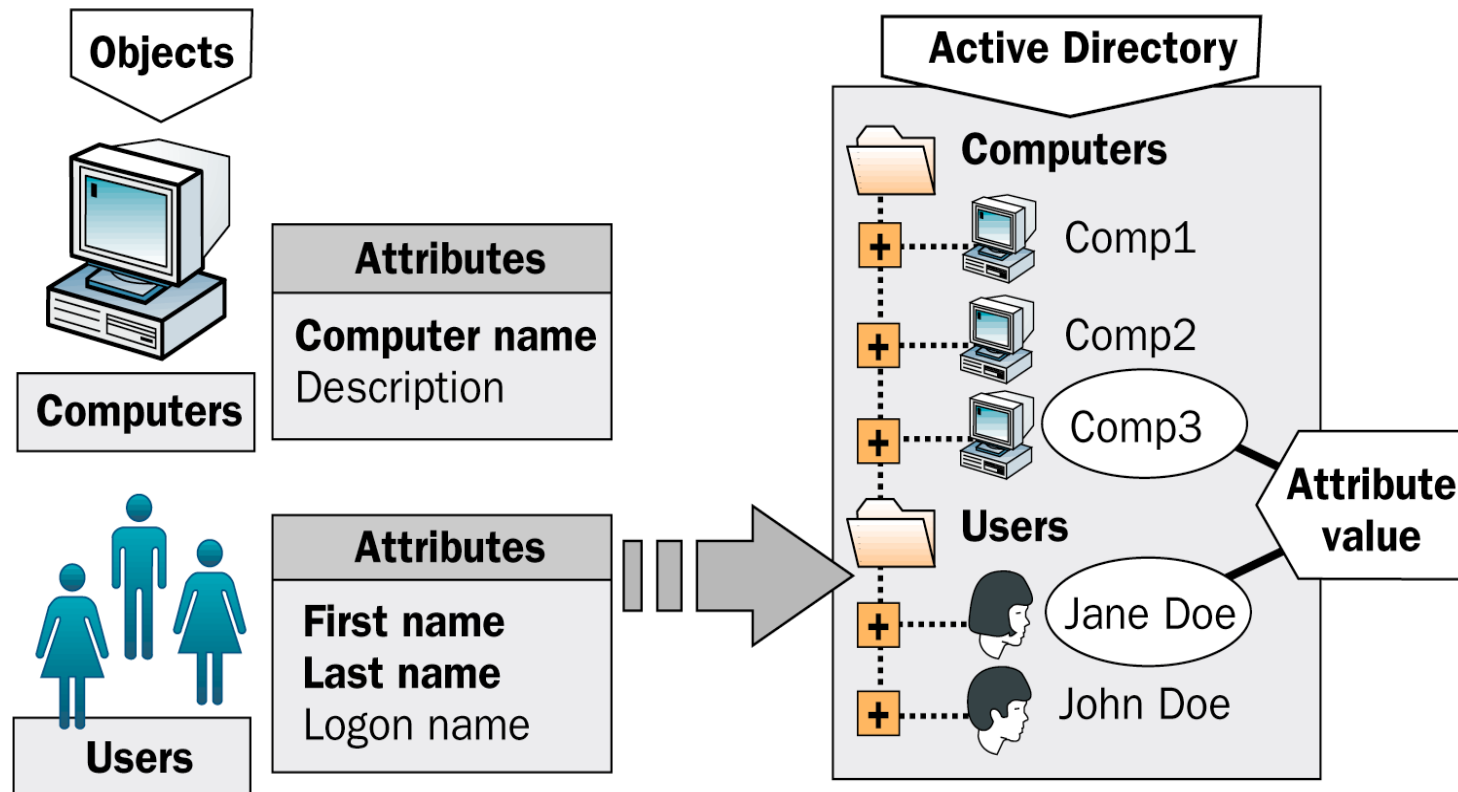


Active Directory Overview

- Active Directory Objects
- Active Directory Components
- Logical Structures
- Physical Structure
- Understanding Active Directory Concepts
- Installation of Domain Controller
- Administering Active Directory
- Creating and Configuring Site Replication
- Backup
- Performance and Monitoring
- Trouble shooting

Active Directory Objects and Attributes



Active Directory Definitions

- Resources stored in the directory, such as user data, printers, servers, databases, groups, computers, and security policies, are known as objects.
- An object is a distinct named set of attributes that represents a network resource.
- Attributes are characteristics of objects in the directory.
- Objects are organized in classes, which are logical groupings of objects.
- Objects known as containers can contain other objects.

Attributes & Classes

Attributes :

- Defined separately from classes
- Defined only once and can be used in multiple classes
- Store the information that describes the object

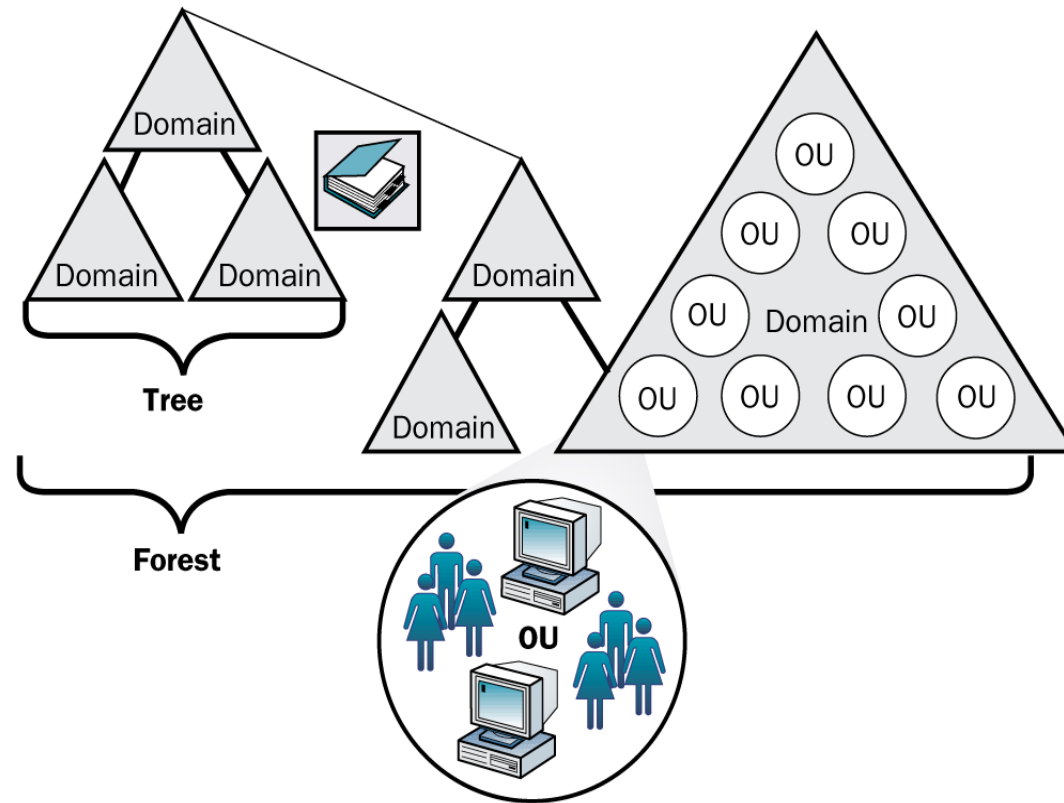
Classes :

- Are collections of attributes.
- Describe the possible objects that can be created.
- Are also referred to as object classes.
- Every object is an instance of an object class.

Active Directory Components

- Logical Structure
 - Domains
 - Organizational units
 - Trees
 - Forests
- Physical Structure
 - Sites
 - Domain controllers

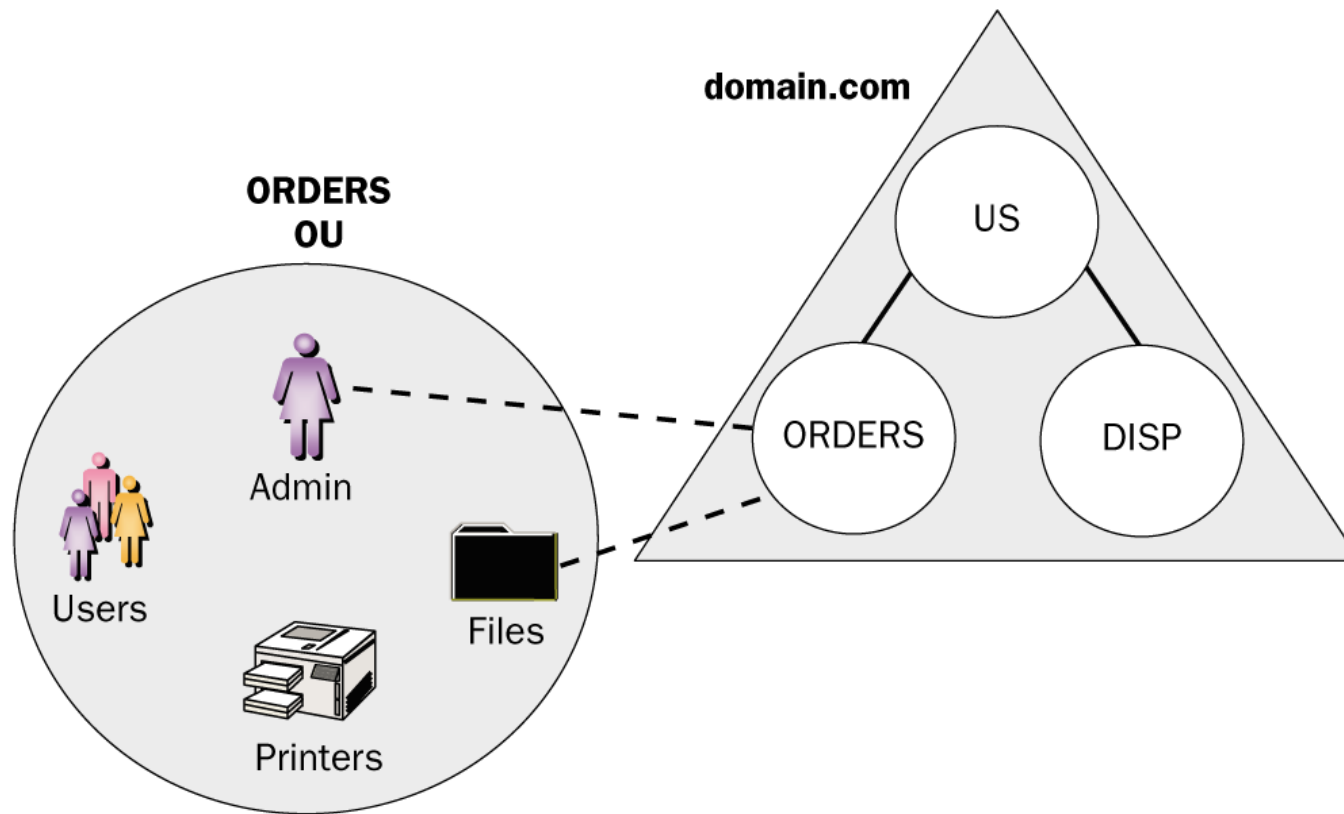
Logical Hierarchical Structure



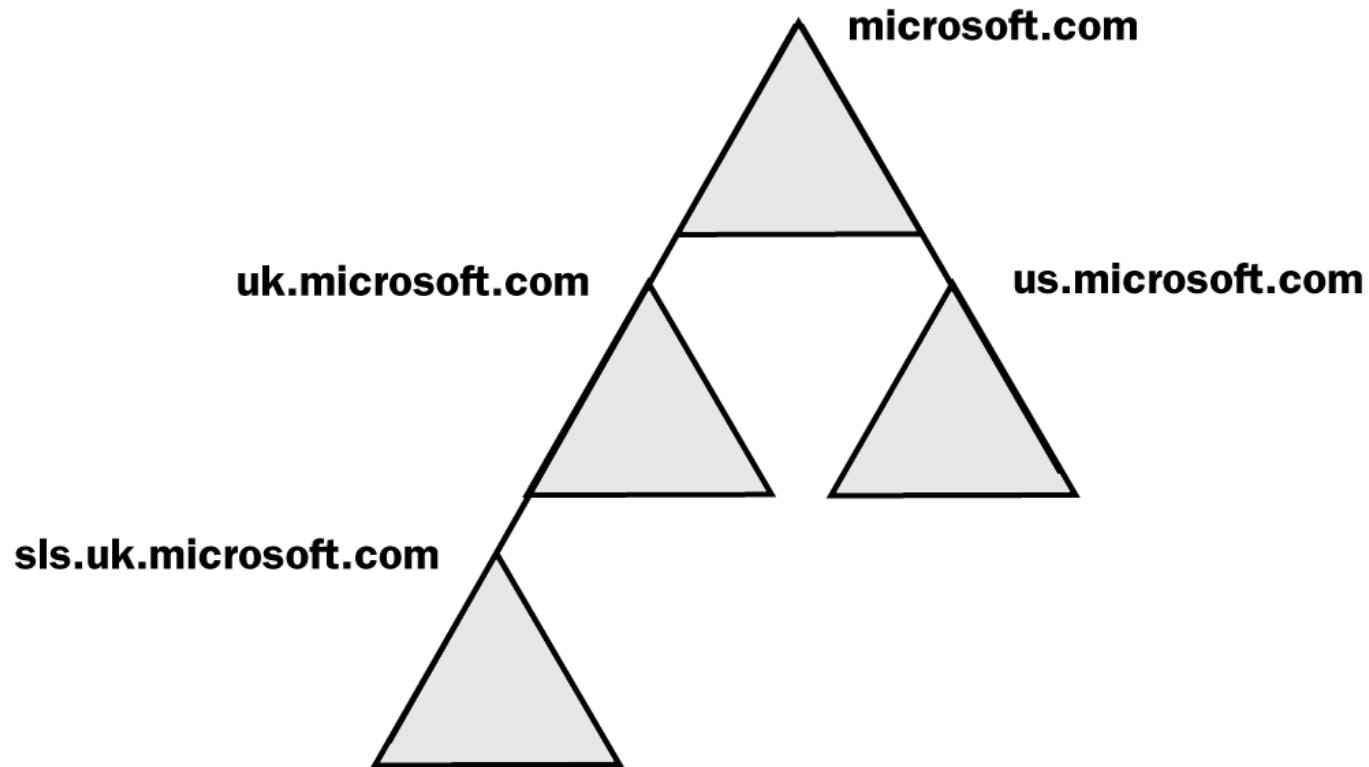
Logical Structure

- Resources should be organized in a logical structure that mirrors the logical structure of the organization.
- Grouping resources logically enables users and administrators to find resources by name rather than by physical location.
- The network's physical structure is transparent to users.

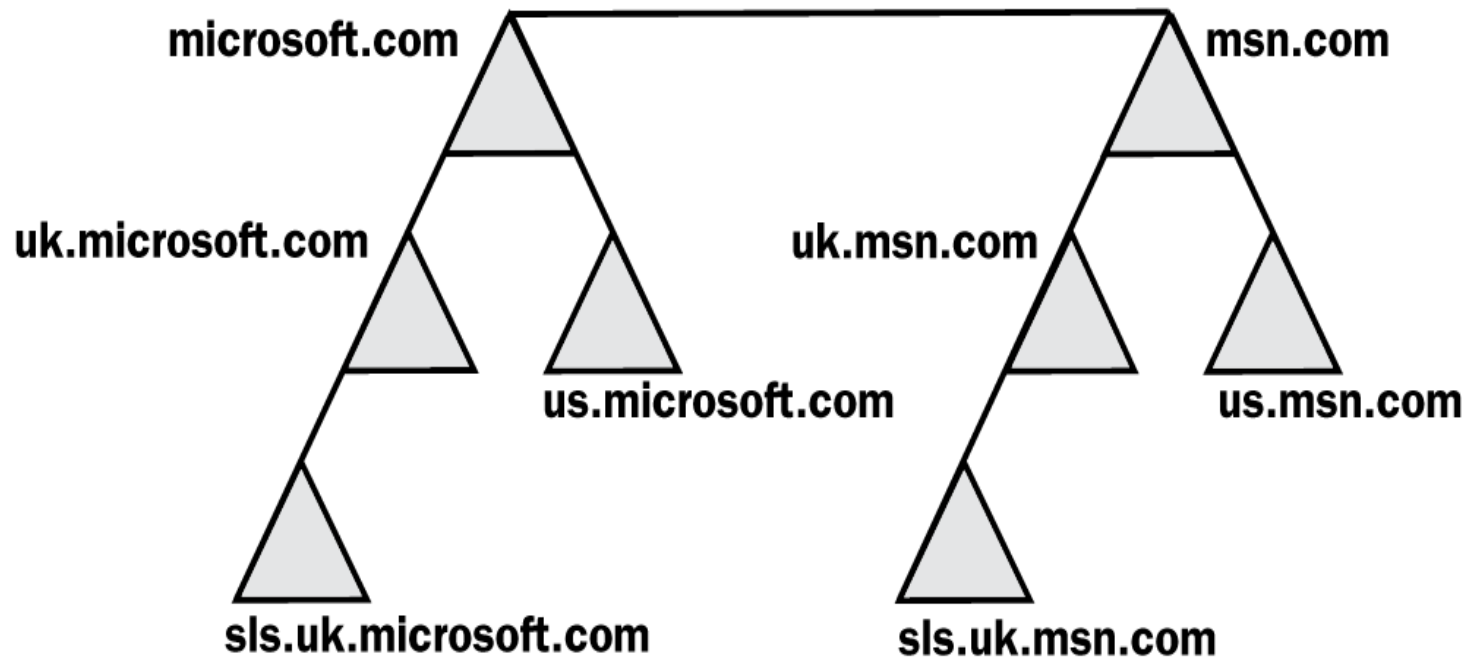
Use OUs to Handle Administrative Tasks



Domain Tree



Forest of Trees



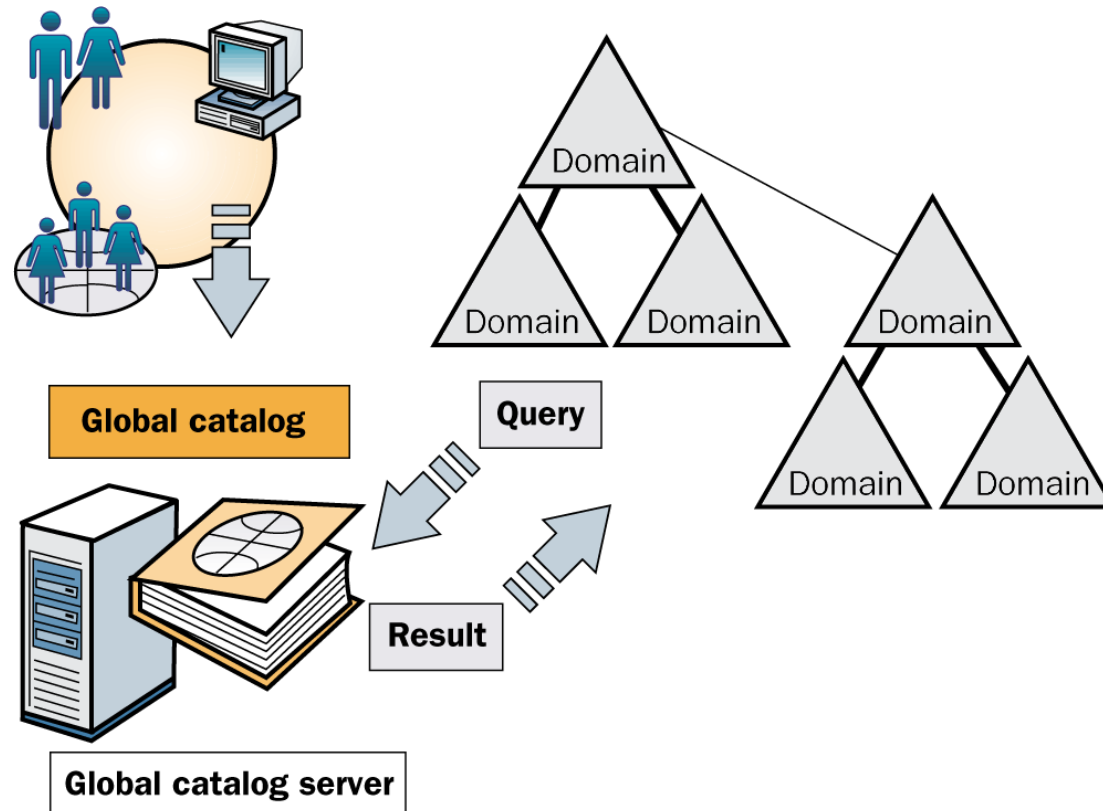
Sites

- Combination of one or more IP subnets connected by a highly reliable and fast link to localize as much network traffic as possible.
- Typically, has the same boundaries as a LAN.
- When grouping subnets on the network, combine only those subnets that have fast, inexpensive, and reliable network connections with one another.
- Available bandwidth of 128 Kbps or greater is sufficient.
- Not a part of the namespace.
- Contain only computer objects and connection objects used to configure replication between sites.

Understanding Active Directory Concepts

- Global Catalog
- Replication
- Trust Relationships
- DNS Namespace
- Name Servers
- Naming Conventions

Global Catalog Is Central Repository



Key Directory Roles

- Enables network logon by providing universal group membership information to a domain controller when a logon process is initiated
- Enables finding directory information regardless of which domain in the forest actually contains the data

Universal Group Membership

- If only one domain controller exists in the domain, the domain controller and the global catalog are the same server.
- If multiple domain controllers exist on the network, the global catalog is the domain controller configured as such.
- If a global catalog is not available when a user initiates a network logon process, the user is able to log on to the local computer only.

Directory Partitions

- Schema information
 - Defines the objects that can be created in the directory and the attributes associated with those objects.
- Configuration information
 - Describes the logical structure of the deployment, containing information such as domain structure or replication topology.
 - Common to all domains in the domain tree or forest.
- Domain data
 - Describes all of the objects in a domain.
 - Domain-specific and not distributed to any other domains.
 - A subset of the properties for all objects in all domains is stored in the global catalog.

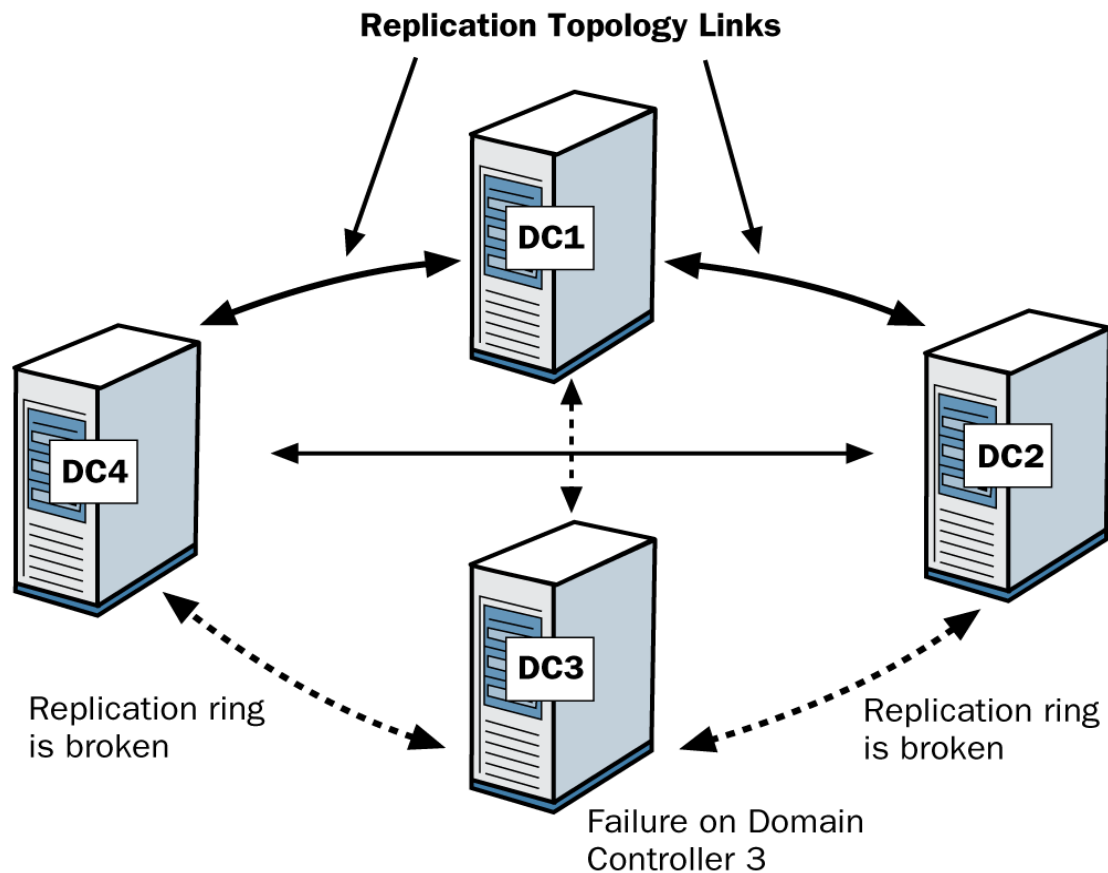
A Domain Controller Stores and Replicates

- Schema information for the domain tree or forest
- Configuration information for all domains in the domain tree or forest
- All directory objects and properties for its domain
- A subset of the properties of all objects in the domain (replicated to the global catalog)

A Global Catalog Stores and Replicates

- Schema information for a forest
- Configuration information for all domains in a forest
- A subset of the properties for all directory objects in the forest (replicated between global catalog servers only)
- All directory objects and all their properties for the domain in which the global catalog is located

Replication Topology



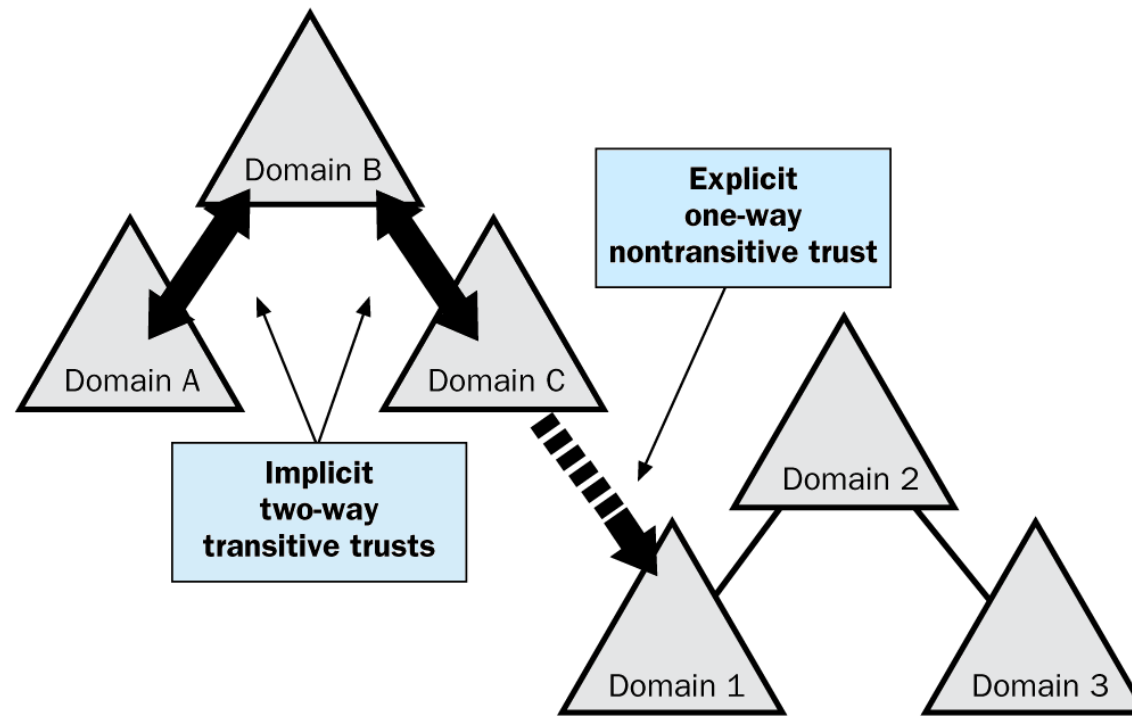
Replication Within a Site

- Active Directory automatically generates a topology for replication among domain controllers in the same domain using a ring structure.
- Topology defines the path for directory updates to flow from one domain controller to another until all domain controllers receive the directory updates.
- Ring structure ensures that at least two replication paths exist from one domain controller to another.
- Active Directory periodically analyzes the replication topology within a site to ensure that it is still efficient.
- If a domain controller is added or removed from the network or a site, Active Directory reconfigures the topology to reflect the change.

Replication Between Sites

- To ensure replication between sites, Active Directory must be customized to replicate information using site links to represent network connections.
- Active Directory uses the network connection information to generate connection objects that provide efficient replication and fault tolerance.
- Information is provided about the replication protocol used, cost of a site link, times when the link is available for use, and how often the link should be used.
- Active Directory uses this information to determine which site link will be used to replicate information.

Two Types of Trust Relationships



Implicit Two-Way Transitive Trust

- Trust relationship between parent and child domains within a tree and between the top-level domains in a forest.
- Established and maintained automatically.
- Feature of the Kerberos authentication protocol.
- If Domain A trusts Domain B, and Domain B trusts Domain C, then Domain A trusts Domain C.

Explicit One-Way Nontransitive Trust

- Trust relationship between domains that are not part of the same tree
- Bounded by the two domains in the trust relationship and does not flow to any other domains in the forest
- This is the only form of trust possible with
 - A Microsoft Windows 2000 domain and a Windows NT domain.
 - A Windows 2000 domain in one forest and a Windows 2000 domain in another forest.
 - A Windows 2000 domain and an MIT Kerberos V5 realm.

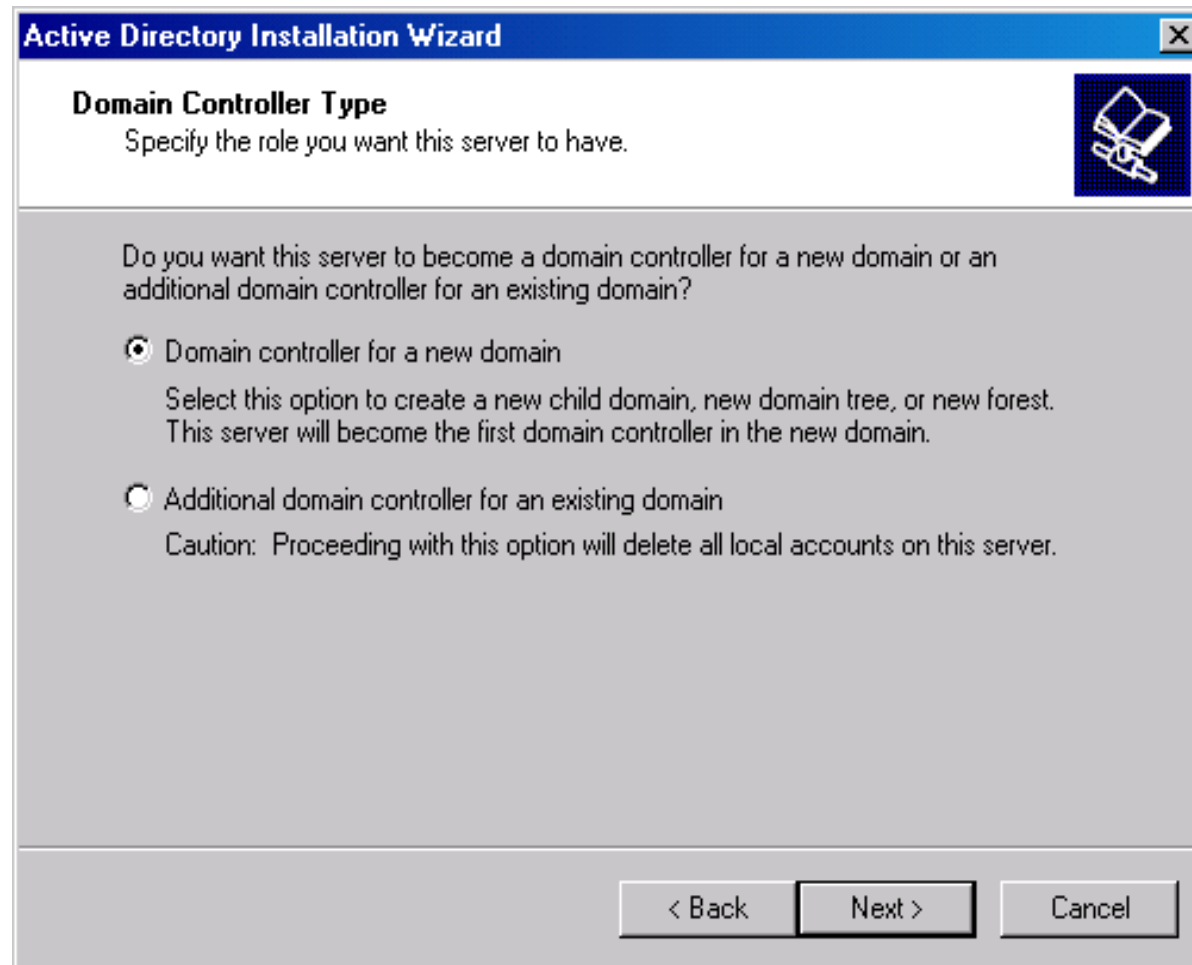
Minimum Requirement to install Active Directory

- For Operating system Windows 2000 Server
- Processor Pentium II 233 Mhz
- RAM 64 MB.
- Hard disk Space 650 MB + (250MB)

200 MB for NTDS

50 MB for Log files

Introduction to the Active Directory Installation Wizard

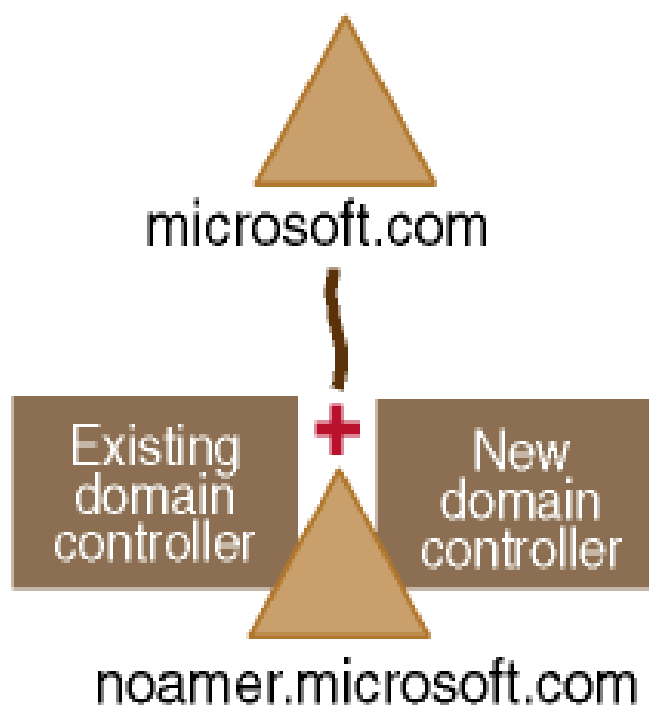


Adding or Creating a Domain Controller

- If you add a domain controller to an existing domain, you create a peer domain controller.
- If you create the first domain controller for a new domain, you are creating not only the domain controller but also a new domain.

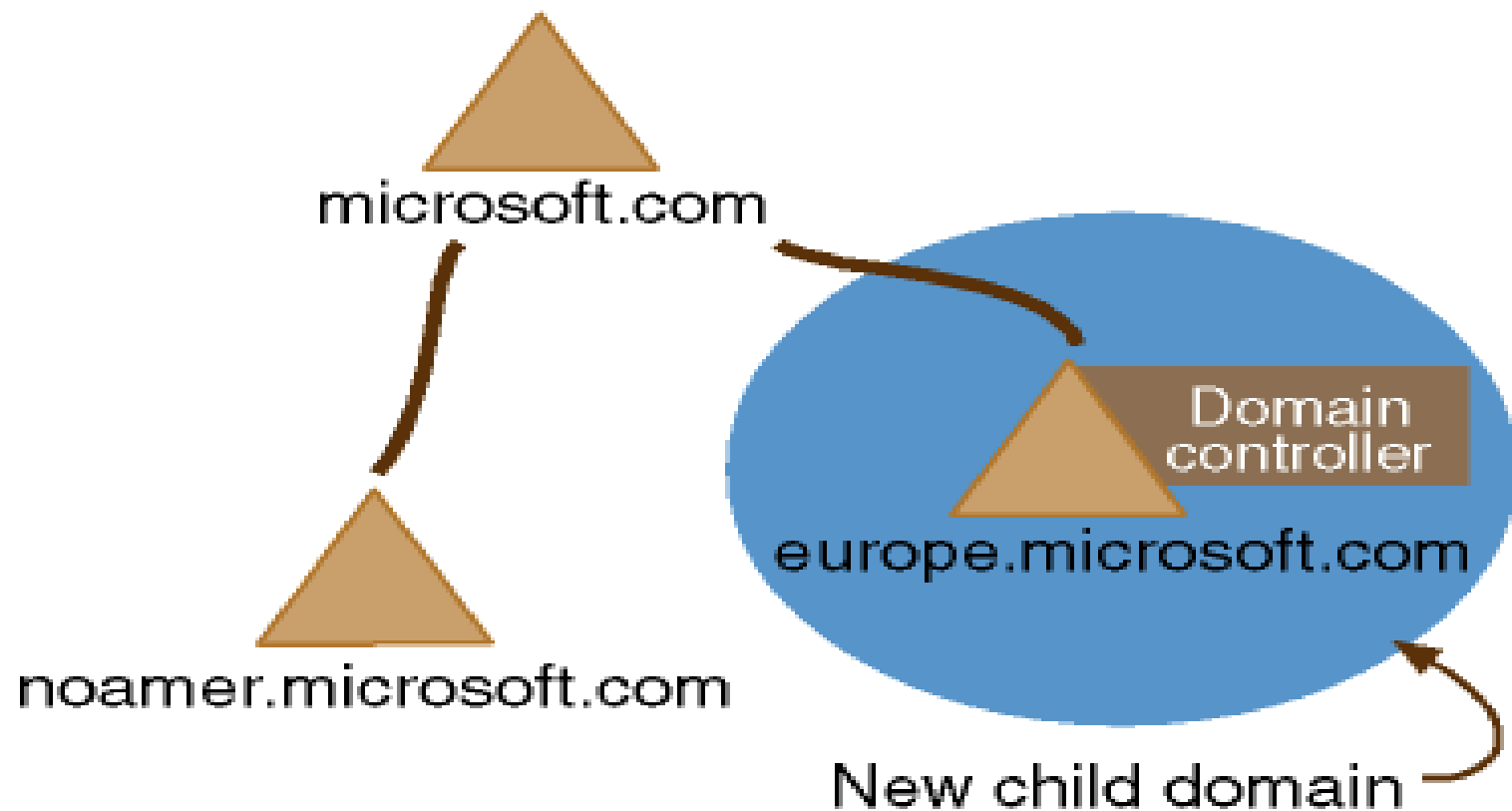
Adding a Domain Controller to an Existing Domain

Additional domain controller for an existing domain

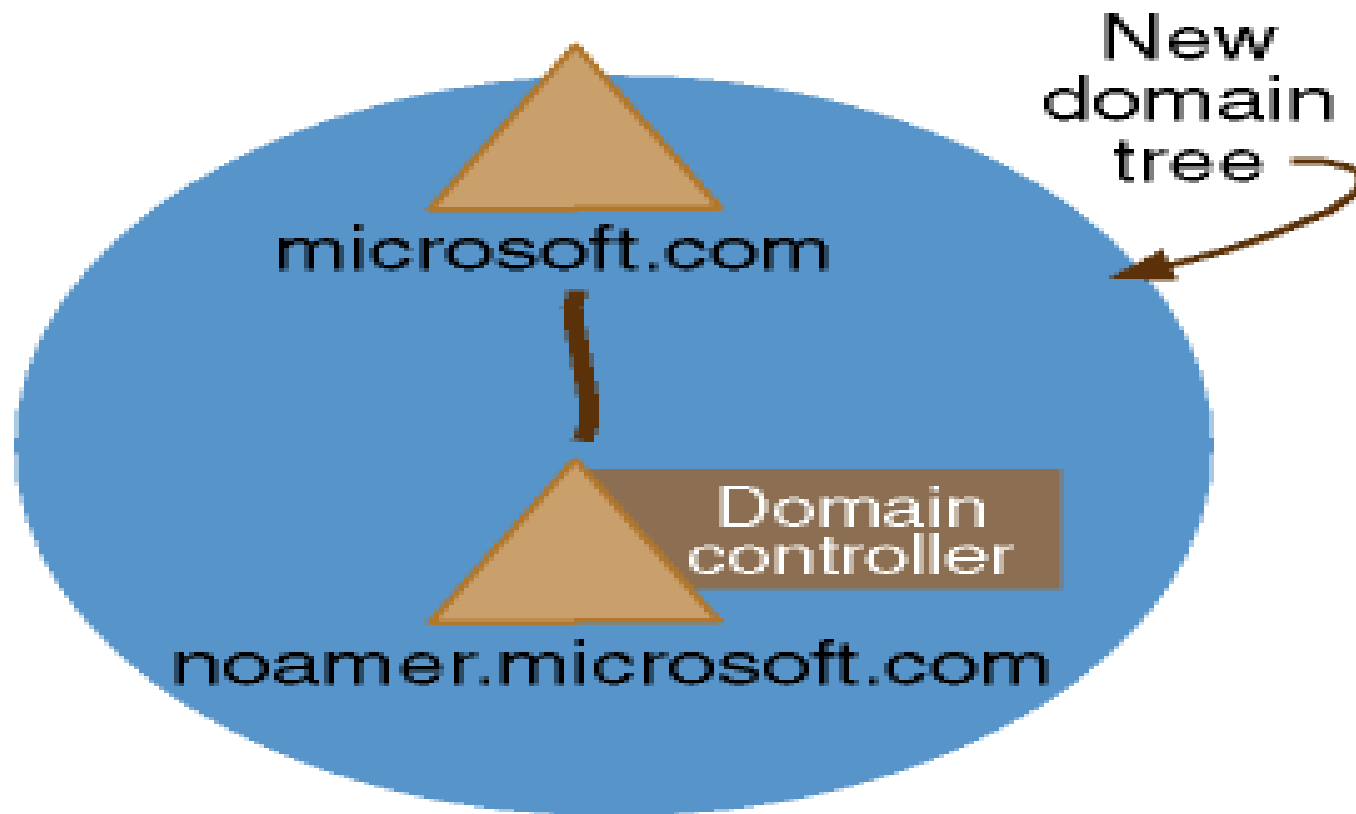


Creating a New Child Domain

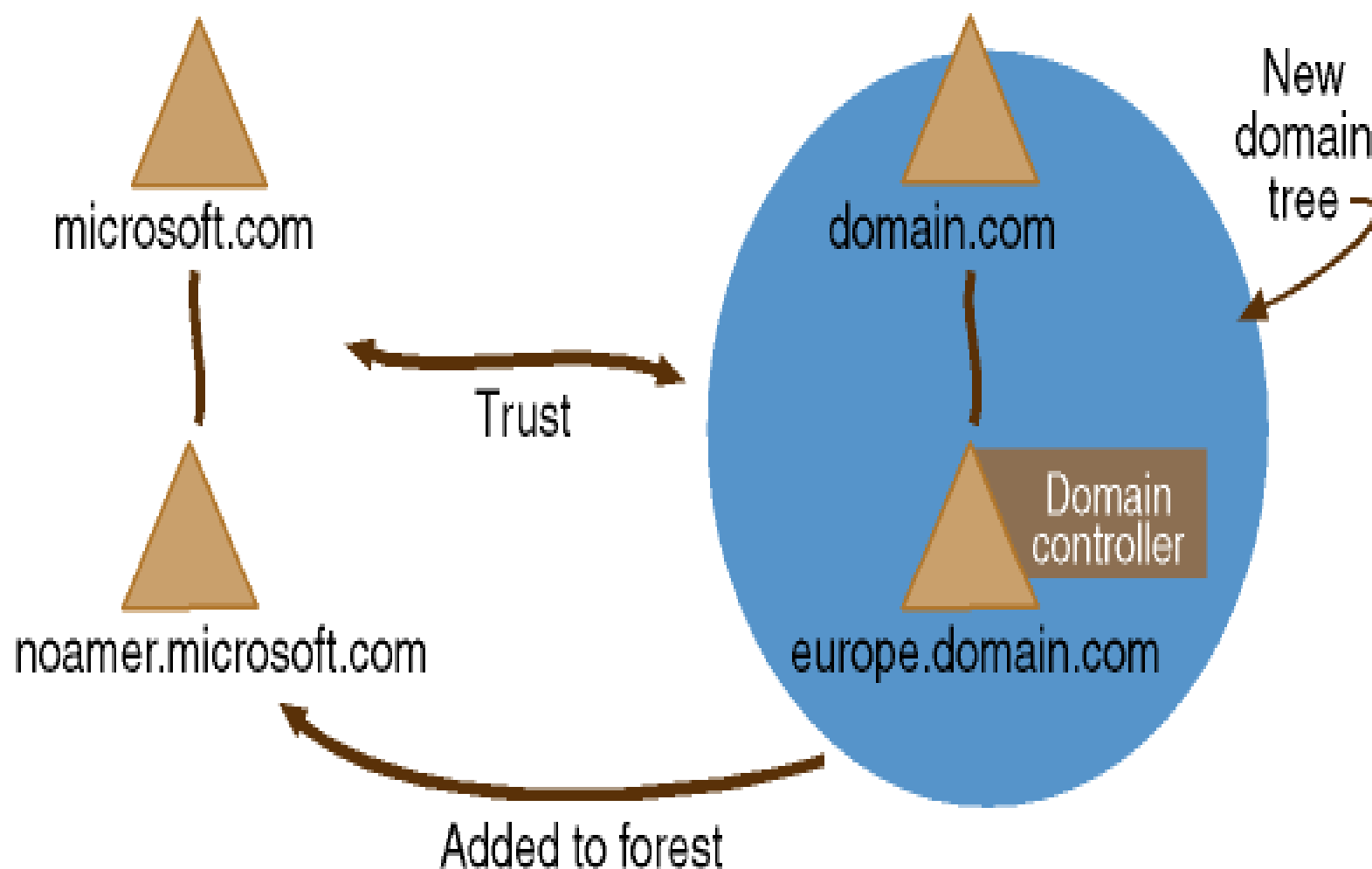
Domain controller for a new domain



Creating a New Domain Tree



Adding a Domain Tree to a Forest



The Active Directory Database

- The database is a file named Ntds.dit, which is the directory for the new domain.
- The default location for the database and the database log files is %systemroot%\Ntds, although you can specify a different location.
- The database contains all the information stores in the Active Directory store.
- The Ntds.dit file is an ESE database that contains the entire schema, the global catalog, and all the objects stored on that domain controller.

The Shared System Volume

- The shared system volume is a folder structure that exists on all Windows 2000 domain controllers.
- The shared system volume stores scripts and some of the group policy objects for the current domain as well as the enterprise.
- Replication of the shared system volume occurs on the same schedule as Active Directory replication.

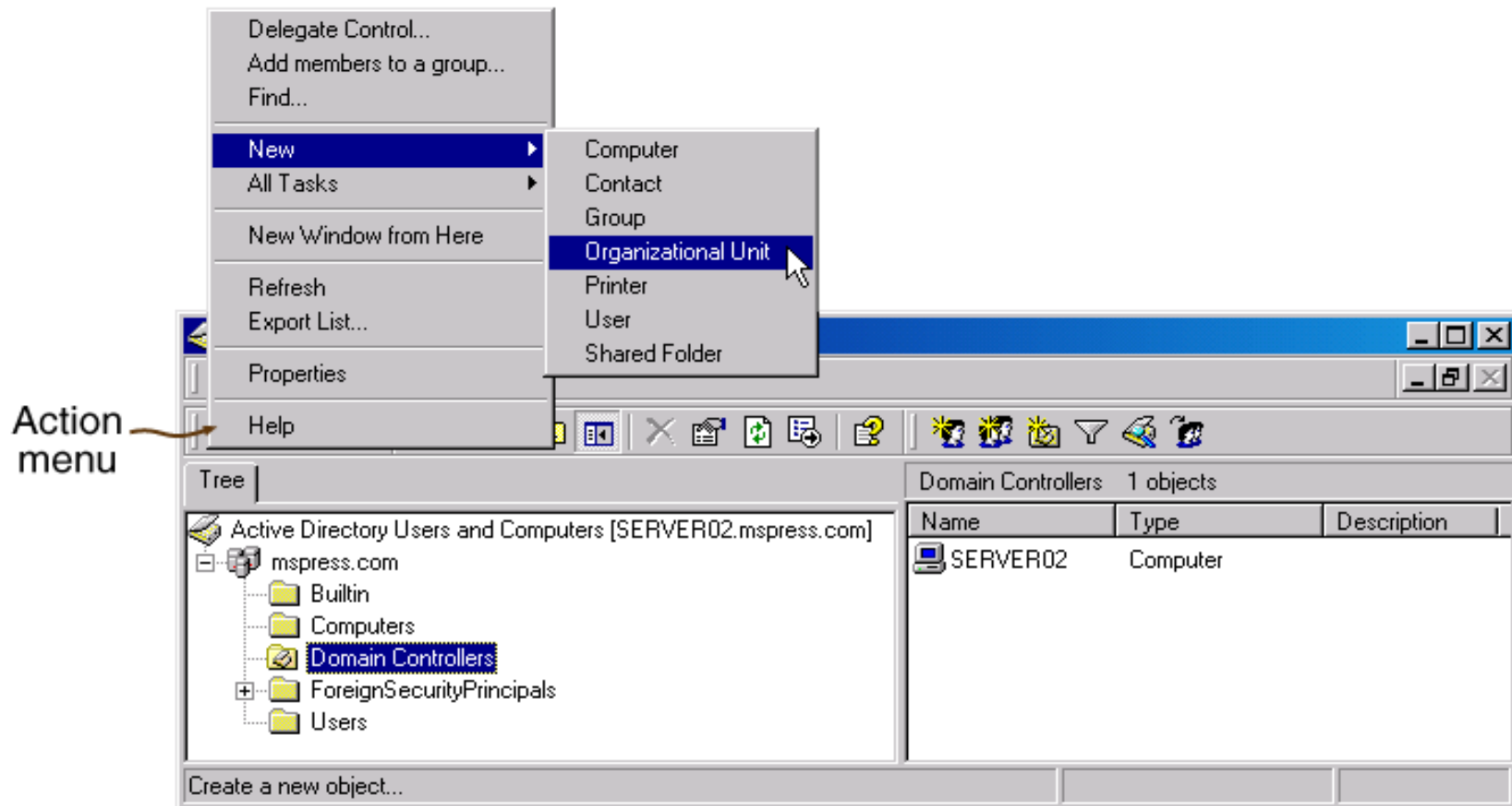
Domain Modes

- Mixed mode (By Default)
- Native mode

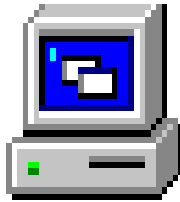
Introduction to OUs and their Objects

- Each Active Directory object is a distinct named set of attributes that represents a specific network resource.
- Before objects are added to Active Directory services, you should create the OUs that will contain those objects.

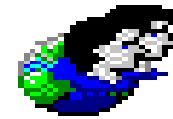
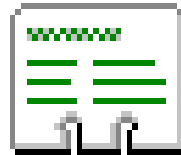
Creating Ous



Adding Objects to OUs

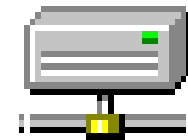
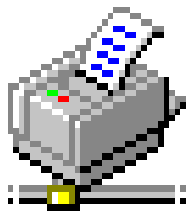


Computer



Group

Group



Locating Objects

Find Users, Contacts, and Groups

File Edit View Help

Find: Users, Contacts, and Groups In: Domain Controllers Browse...

Users, Contacts, and Groups Advanced

Name: John

Description:

Find Now
Stop
Clear All

Name	X500 Distinguished Name	Type
John Numbercrunch	CN=John Numbercrunch,OU=Accounting,OU=Domain Controllers,DC=mspress,DC=com	Contact
John Smiles	CN=John Smiles,OU=Public Relations,OU=Domain Controllers,DC=mspress,DC=com	User
John q. Seller	CN=John q. Seller,OU=Marketing,OU=Domain Controllers,DC=mspress,DC=com	User
John Smith	CN=John Smith,OU=Accounting,OU=Domain Controllers,DC=mspress,DC=com	User
John Doe	CN=John Doe,OU=Human Resources,OU=Domain Controllers,DC=mspress,DC=com	User

5 item(s) found

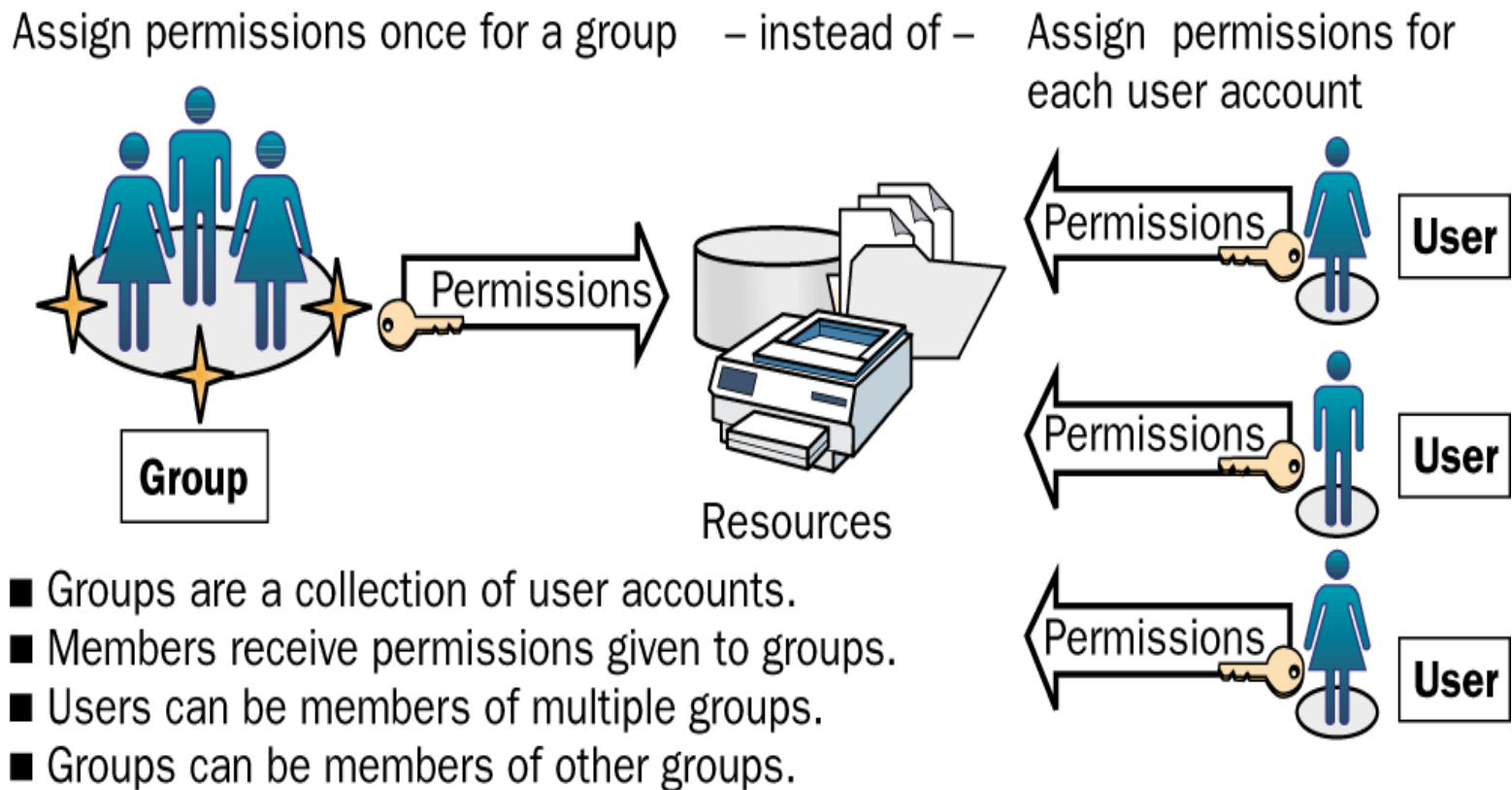
Modifying Attributes and Deleting Objects

- You can modify the attributes of an object to change or add information.
- You can modify an object's attribute by opening the properties for that object in the Active Directory Users And Computers snap-in.
- To maintain security, delete objects when they are no longer needed.

Moving Objects

- You can move objects from one location in the Active Directory store to another location.
- You should move objects when organization or administrative functions change.

Groups Simplify Administration



Group Types

- Two group types exist: security and distribution.
- The group type determines how the group is used.
- Both types are stored in the database component of Active Directory.
- Storage in the database component allows use of groups anywhere in the network.

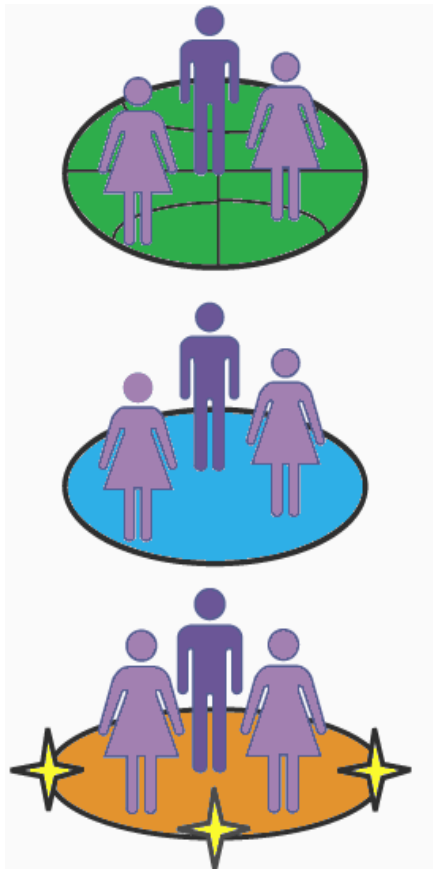
Security Groups

- Microsoft Windows 2000 uses only security groups.
- Security groups are used to assign permissions to gain access to resources.
- A security group has all the capabilities of a distribution group.

Distribution Groups

- Used by applications as lists for nonsecurity-related functions
- Used when the only function of the group is nonsecurity-related
- Cannot be used to assign permissions

Group Scopes



Global group

Members come only from local domain.
Members can access resources in any domain.

Domain local group

Members can come from any domain.
Members access resources only in local domain.

Universal group

Members can come from any domain.
Members can access resources in any domain.

Group Scope Overview

- A group type and scope must be selected when a group is created.
- Group scopes allow groups to be used in different ways to assign permissions.
- The scope of a group determines where in the network the group can be used to assign group permissions.

Global Groups

- Used to organize users who share similar network access requirements.
- Members can be added only from the domain in which the global group is created.
- Can be used to assign permissions to gain access to resources that are located in any domain in the domain tree or forest.

Domain Local Groups

- Used to assign permissions to resources.
- Members can be added from any domain.
- Can be used to assign permissions to gain access to resources located only in the same domain where the domain local group is created.

Universal Groups

- Used to assign permissions to related resources in multiple domains.
- Members can be added from any domain.
- Can be used to assign permissions to gain access to resources located in any domain.
- Not available in mixed mode.
- Full feature set of Windows 2000 is available only in native mode.

Groups for Administrators

- Why You Should Not Run Your Computer as an Administrator
- Administrators as Members of the Users and Power Users Groups
- Using Run As to Start a Program
- RUNAS Command
- RUNAS Examples
- Practice: Using Run As to Start a Program as an Administrator

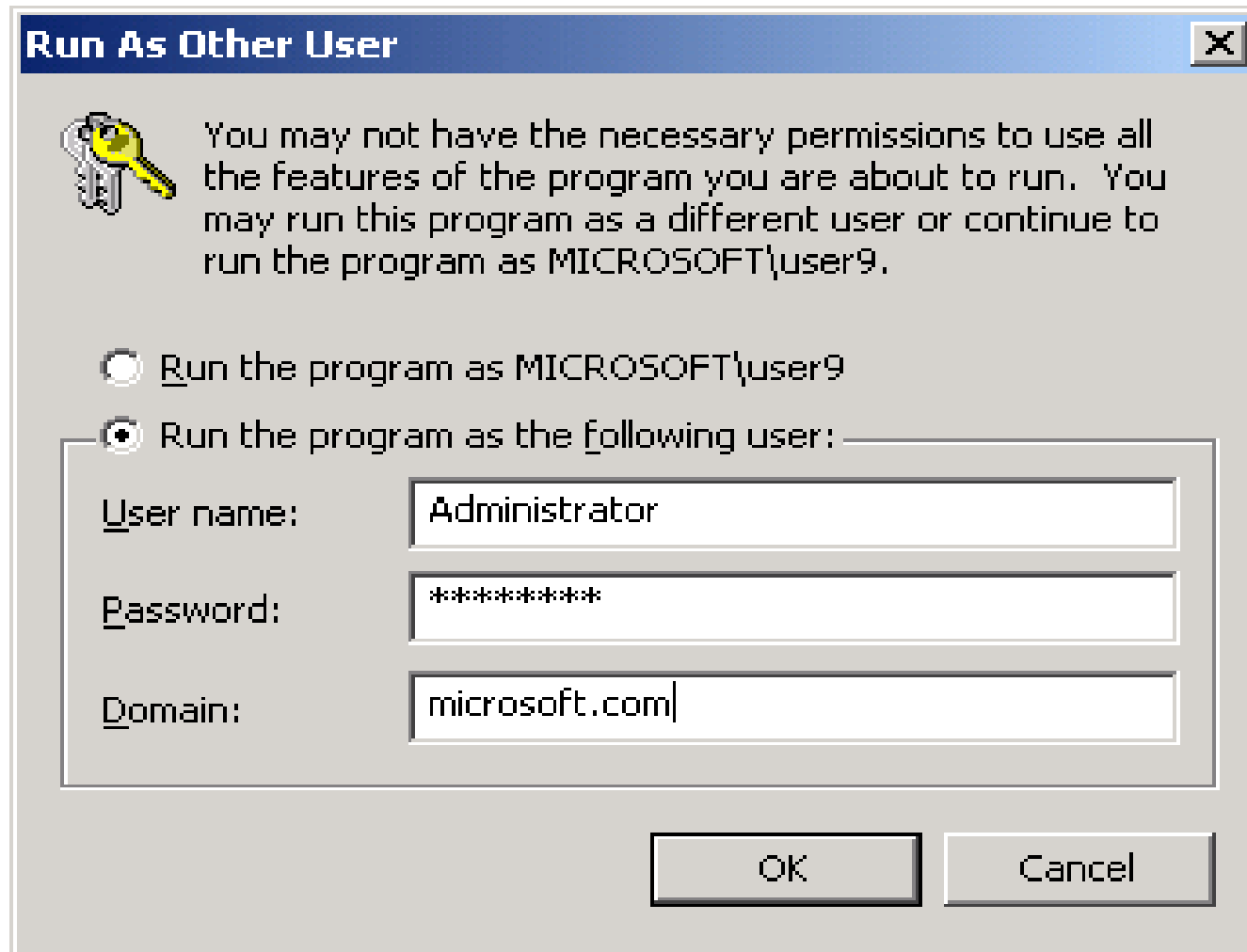
Using Run As to Start a Program

- Run As is used to run a program that requires the user to be logged on as an administrator.
- Run As allows one to run administrative tools with either local or domain administrator rights and permissions while logged on as a normal user.
- If you attempt to start a program, MMC console, or Control Panel item from a network location using the Run As program, it might fail if the credentials used to connect to the network share are different from the credentials used to start the program.
- Credentials used to run the program may not be able to gain access to the same network share.

Using Run As to Start a Program (con't)

- The RunAs service must be running for Run As to start a program.
- The RunAs service can be configured to start automatically when the system starts using the RunAs Server option in the Services console.
- A property should be set on shortcuts to programs and MMC tools so that you will always be prompted for alternate credentials when you use the shortcut.
 - A property is set by right-clicking the shortcut, clicking Properties, and then clicking the Run As Different User check box.
 - When the shortcut is started, the Run As Other User dialog box appears, prompting for the alternate user name, password, and domain.

Run As Other User Dialog Box



Creating Sites and Subnets

- Replication is an important function of the Active Directory service.
- All domain controllers must have an identical copy of the Active Directory database.
- In most cases replication is automatic, but sometimes you must create Active Directory objects needed to manually configure replication.

Configuring Site Settings

- To configure a site setting:
 1. Create a new site object.
 2. Associate a subnet with the site.
 3. Connect the sites using site links.

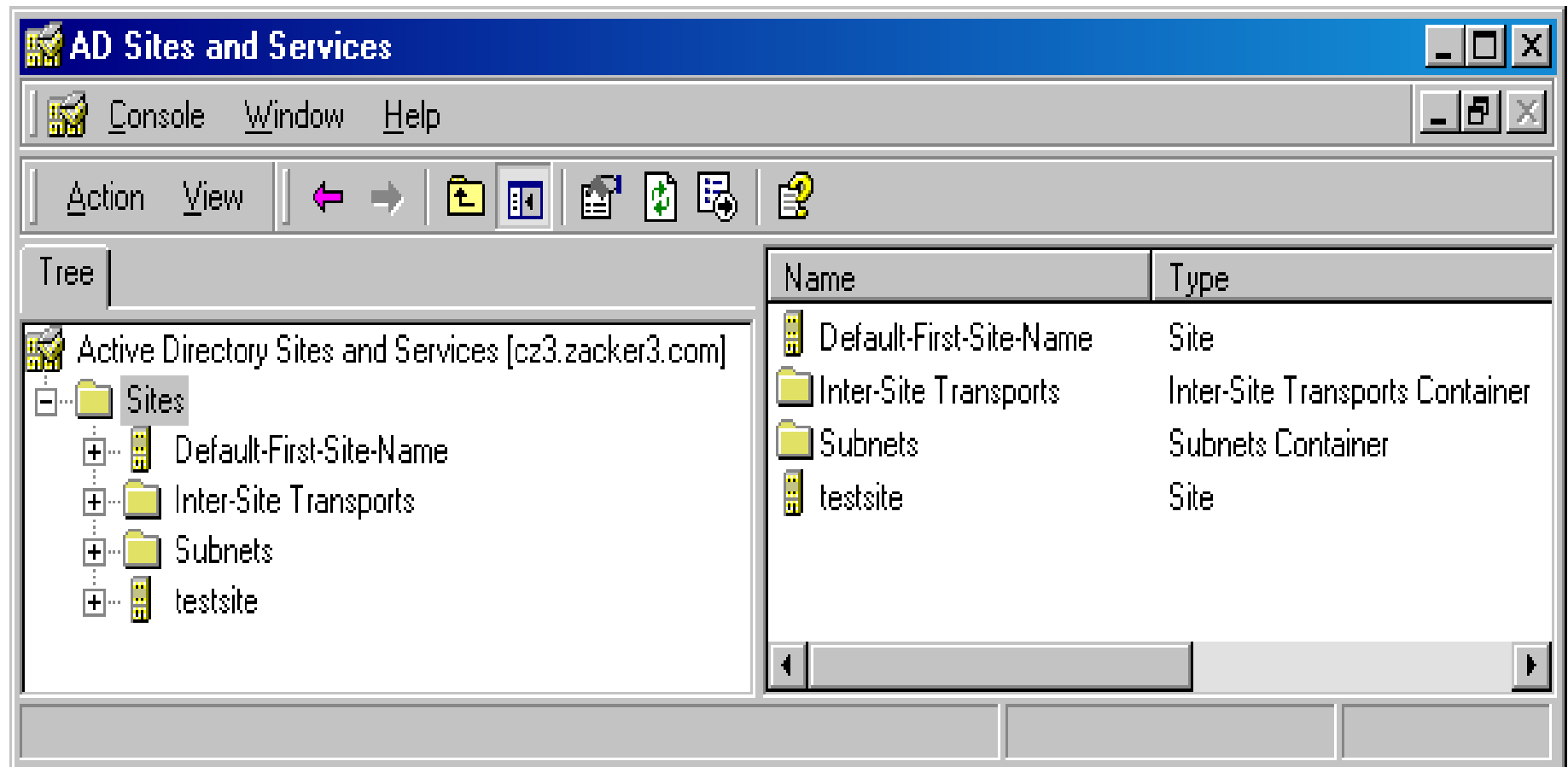
Creating a Site Object

- In Active Directory, a site is a set of servers that are well connected in terms of speed and cost.
 - Well connected usually means the servers are connected using a local area network (LAN) protocol such as Ethernet or Token Ring.
- Replication *within* sites occurs as needed, when changes are made on a domain controller, rather than as scheduled.

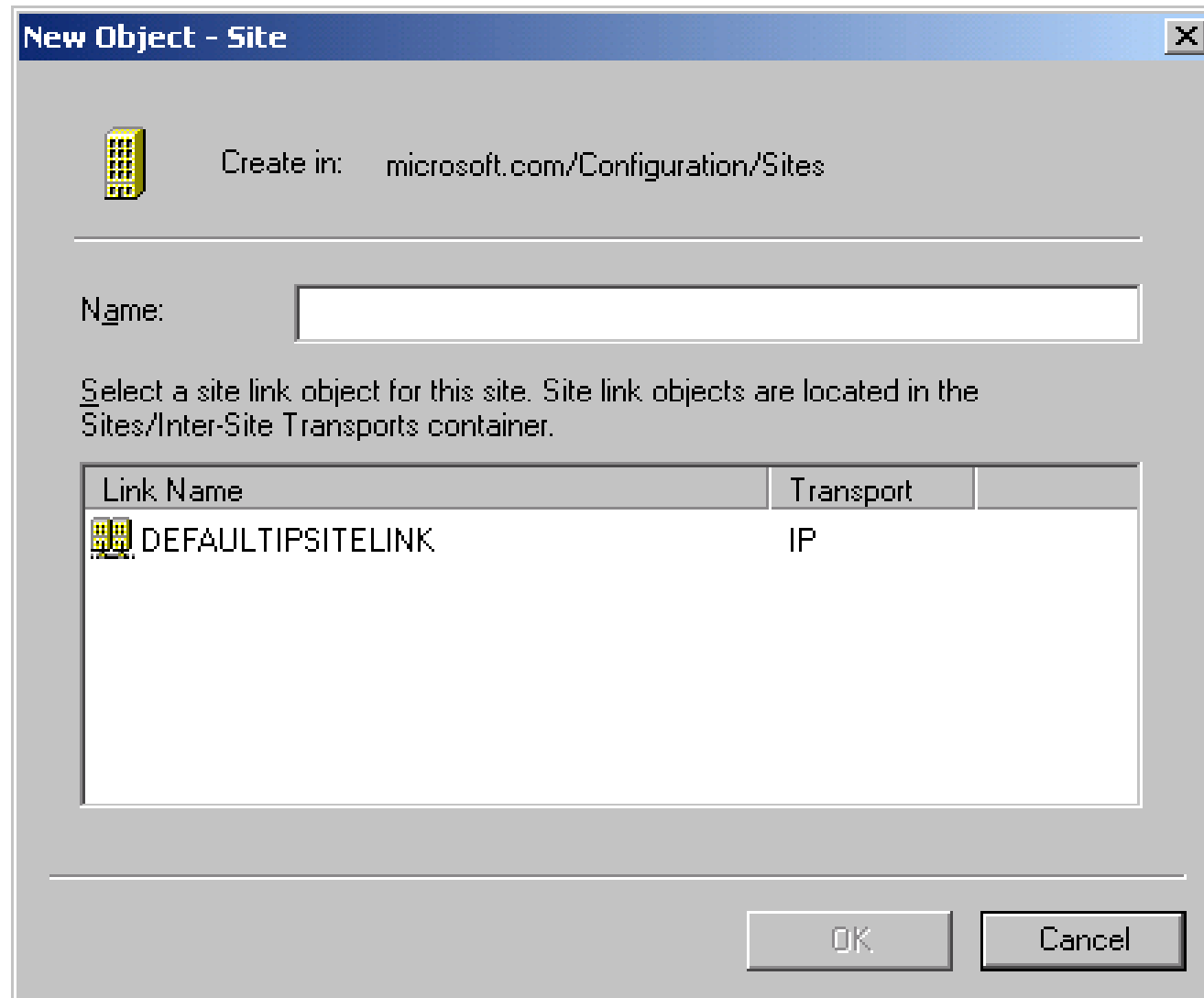
Creating a Site Object (Cont.)

- By default, all domain controllers on an Active Directory network are part of a single site, which is automatically created by Microsoft Windows 2000 when the first domain is created.
- You can create additional sites when domain controllers are connected by slow or costly links, such as wide area network (WAN) links.
- Replication *between* sites occurs only as scheduled.
- By default, all domain controllers on an Active Directory network are part of a single site, which is automatically created by Microsoft Windows 2000 when the first domain is created.
- You can create additional sites when domain controllers are connected by slow or costly links, such as wide area network (WAN) links.
- Replication *between* sites occurs only as scheduled.

The Active Directory Sites And Services Console



The New Object – Site Dialog Box




The dialog box is titled "New Object - Site" and features a close button (X) in the top right corner. Below the title bar, there is a yellow building icon and the text "Create in: microsoft.com/Configuration/Sites". A horizontal line separates this from the "Name:" label and an empty text input field. Below the input field, a paragraph of text reads: "Select a site link object for this site. Site link objects are located in the Sites/Inter-Site Transports container." Underneath this text is a table with two columns: "Link Name" and "Transport". The table contains one row with a yellow building icon, the text "DEFAULTIPSITELINK", and the text "IP". At the bottom of the dialog box, there are two buttons: "OK" and "Cancel".

Create in: microsoft.com/Configuration/Sites

Name:

Select a site link object for this site. Site link objects are located in the Sites/Inter-Site Transports container.

Link Name	Transport
 DEFAULTIPSITELINK	IP

OK Cancel

Associating a Subnet Object With a Site

- Computers on Transmission Control Protocol/Internet Protocol (TCP/IP)–based Active Directory networks are assigned to sites based on their location in subnets.
- Subnets group computers in a way that identifies their physical proximity on the network.
- A site consists of one or more IP subnets.
- You create subnet objects and associate them with a particular site by using Active Directory Sites And Services.

The New Object – Subnet Dialog Box

New Object - Subnet

Create in: microsoft.com/Configuration/Sites/Subnets

Address:

Mask:

Name:

Enter the subnet address and mask. This will be automatically translated into a subnet name in the form network/bits-masked.
Example: address 10.14.209.14 mask 255.255.240.0 becomes subnet 10.14.208.0/20.

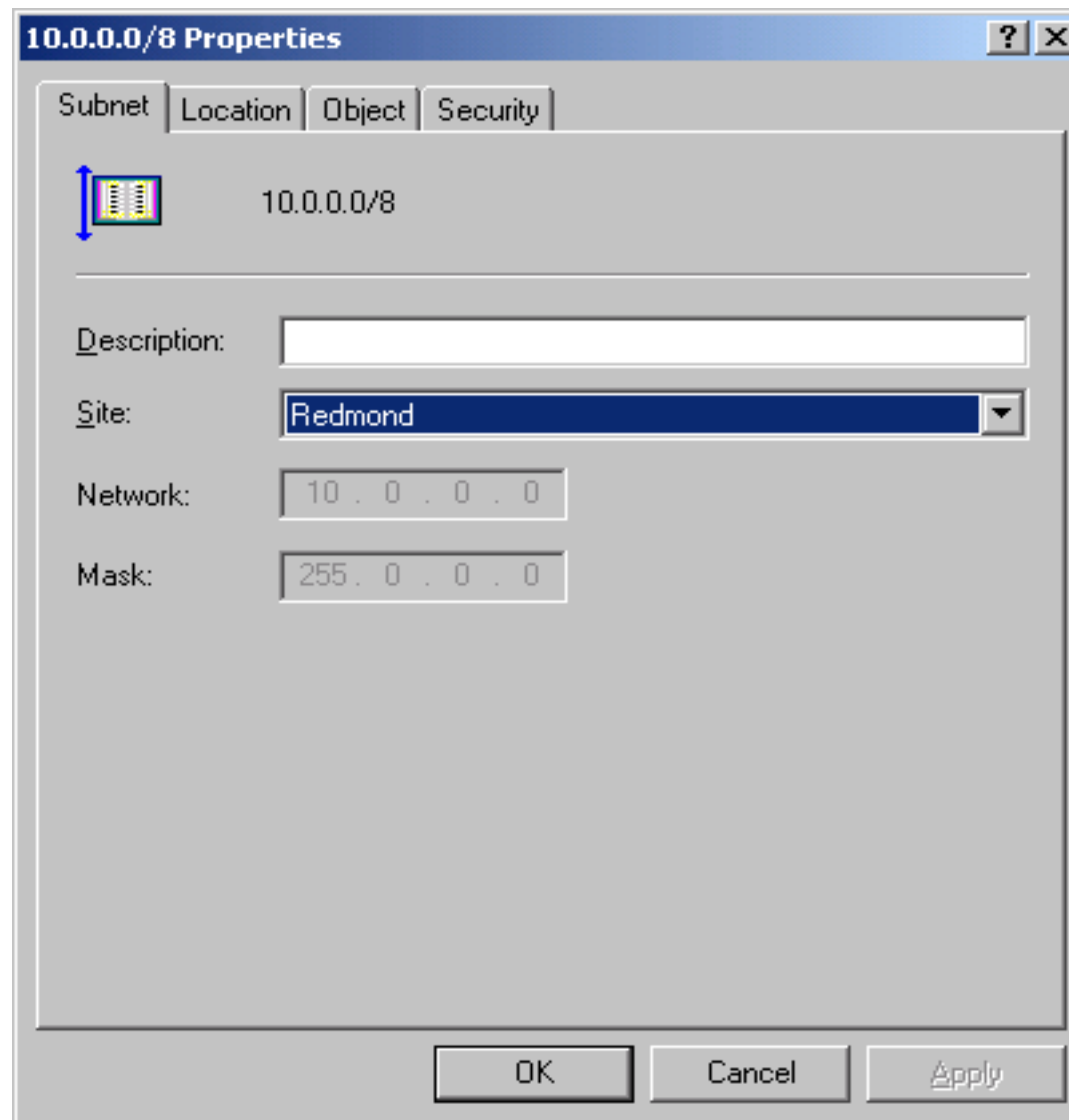
Select a site object for this subnet.

Site Name

- Chicago
- Redmond

OK Cancel

The Properties Dialog Box for a Subnet



Creating Site Links

- A site link object and a physical link (such as a WAN connection) are required for replication to occur between two sites.
- You can configure a site link object to determine when replication between the sites will occur.
- You can use a single site link object to connect more than one pair of sites.
- You create site links by using Active Directory Sites And Services.
- DEFAULTSITE LINK is automatically created in the IP container when you install Active Directory on the first domain controller in the site.
- You can create any additional site links you need.

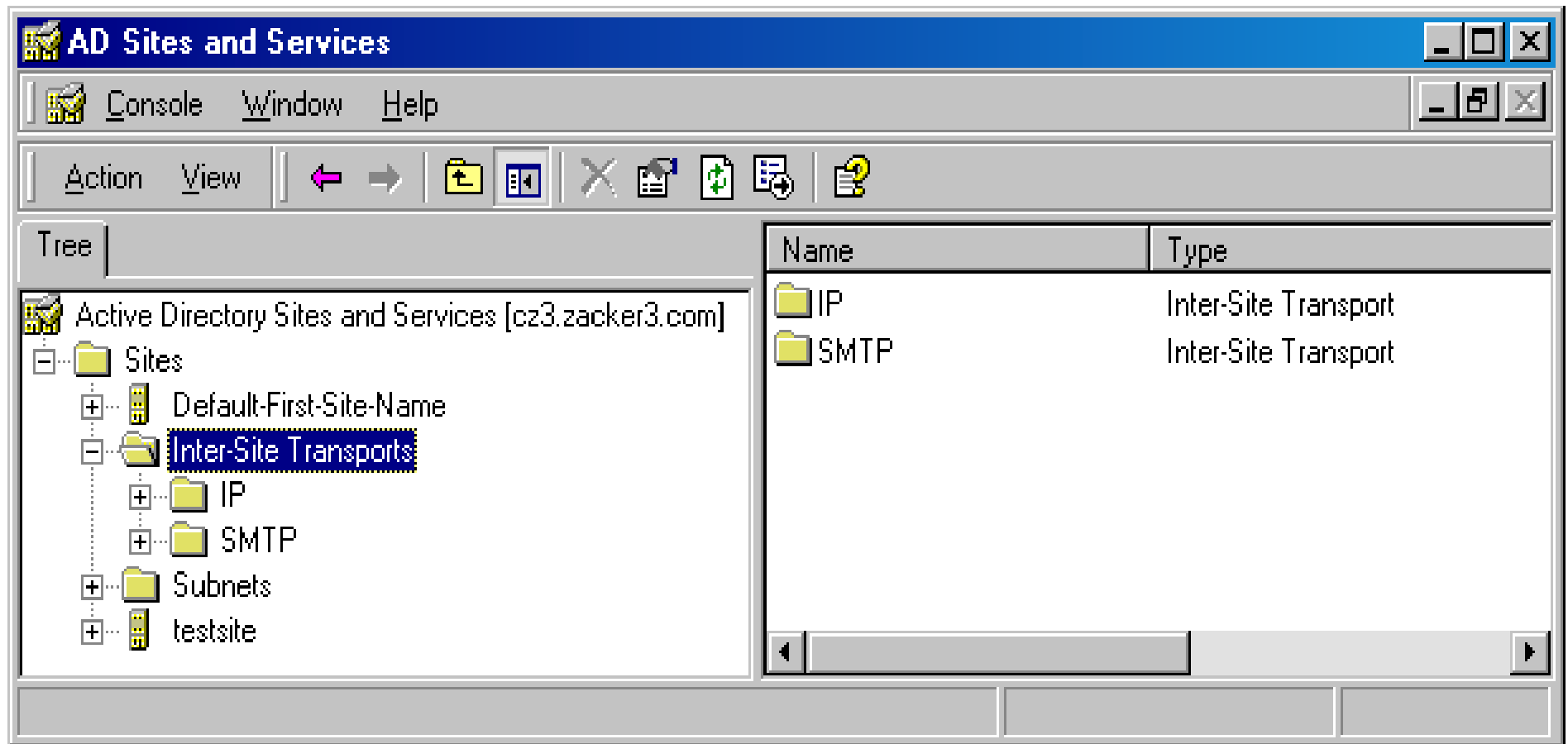
Replication Protocols

- Site link objects use Internet Protocol (IP) or Simple Mail Transfer Protocol (SMTP) to establish connections between sites.
- IP replication
 - Uses remote procedure calls (RPCs) for replication over site links (intersite) and within a site (intrasite)
 - Normally adheres to replication schedules
- SMTP replication
 - Is used only for intersite replication
 - Typically ignores all schedules

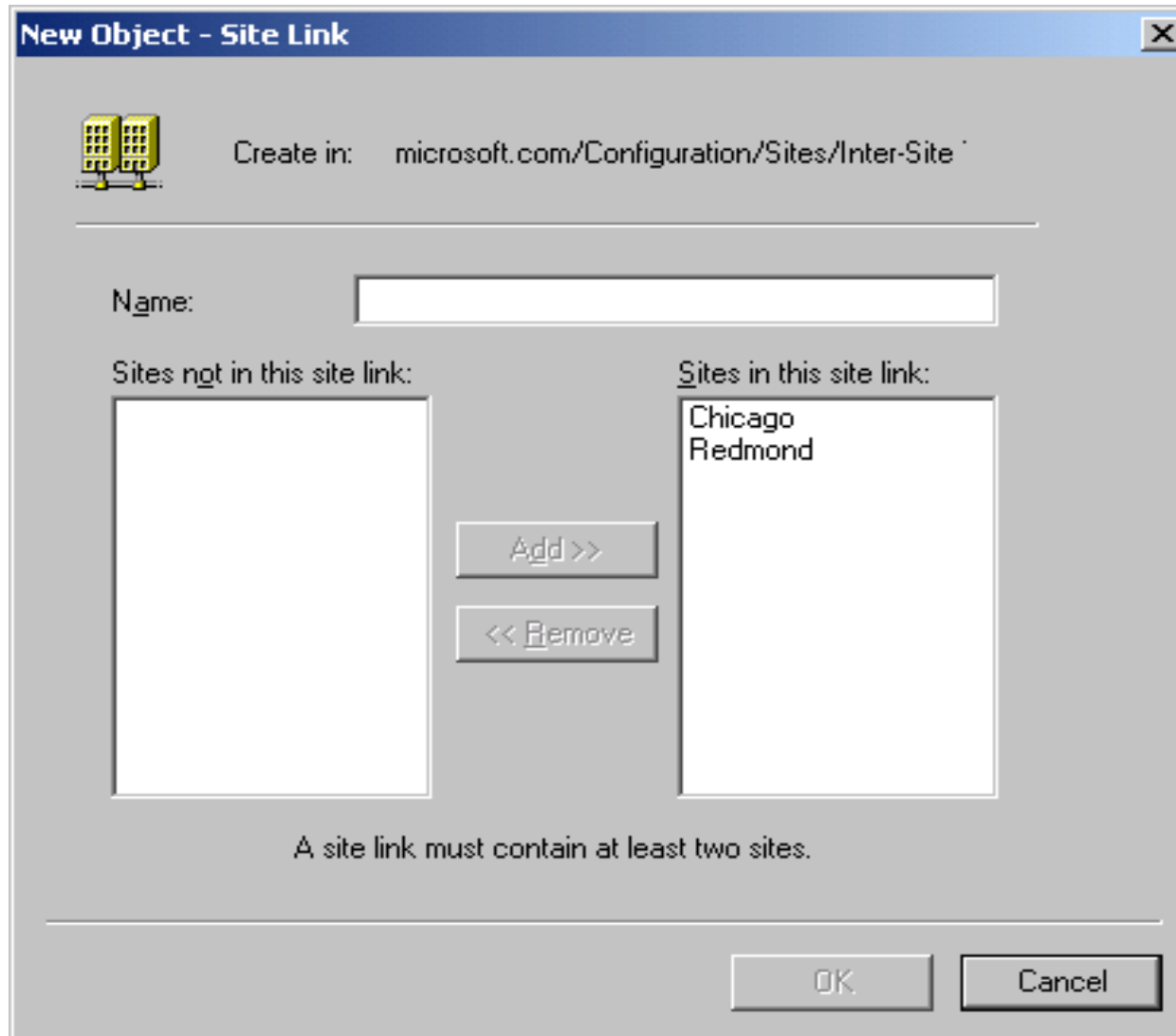
Creating Site Link Objects

- The Inter-Site Transports folder contains the IP folder and the SMTP folder.
- You create site link objects under the folder for the protocol you want that site link to use.

The Inter-Site Transports Folder in Active Directory Sites And Services



The New Object – Site Link Dialog Box



The dialog box is titled "New Object - Site Link" and features a close button (X) in the top right corner. Below the title bar, there is a yellow icon of two buildings and the text "Create in: microsoft.com/Configuration/Sites/Inter-Site". A horizontal line separates this header from the main content area. The main area contains a "Name:" label followed by a text input field. Below this, there are two list boxes: "Sites not in this site link:" on the left and "Sites in this site link:" on the right. The right list box contains the text "Chicago" and "Redmond". Between the two list boxes are two buttons: "Add >>" and "<< Remove". At the bottom of the dialog box, there is a message: "A site link must contain at least two sites." and two buttons: "OK" and "Cancel".

New Object - Site Link

Create in: microsoft.com/Configuration/Sites/Inter-Site

Name:

Sites not in this site link:

Sites in this site link:

Chicago
Redmond

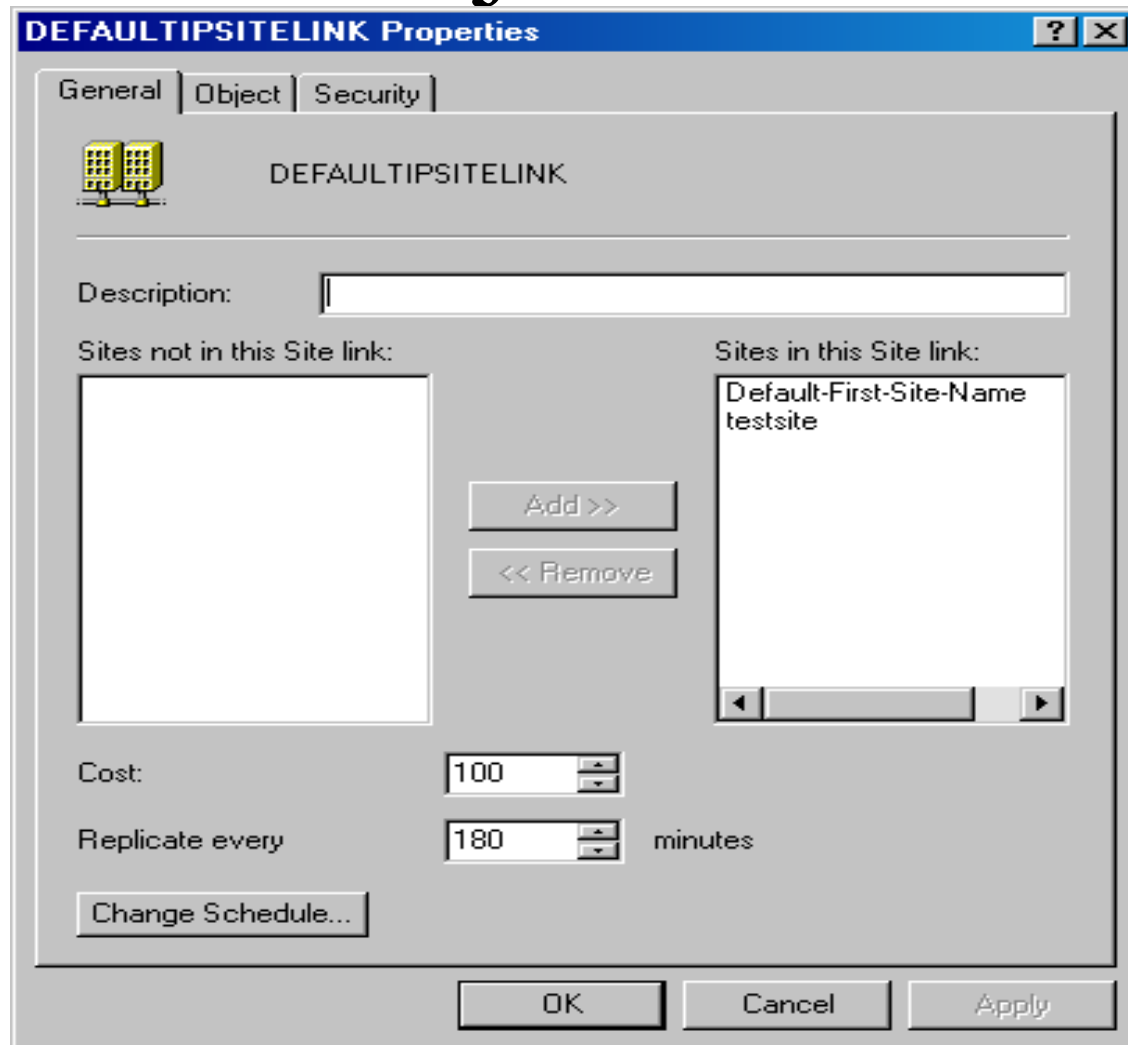
Add >>

<< Remove

A site link must contain at least two sites.

OK Cancel

The Properties Dialog Box for a Site Link Object



Tasks for Configuring Intersite Replication

1. Create site links.
2. Configure site link attributes.
3. Create site link bridges.
4. Configure connection objects (optional).
5. Designate a preferred bridgehead server (optional).

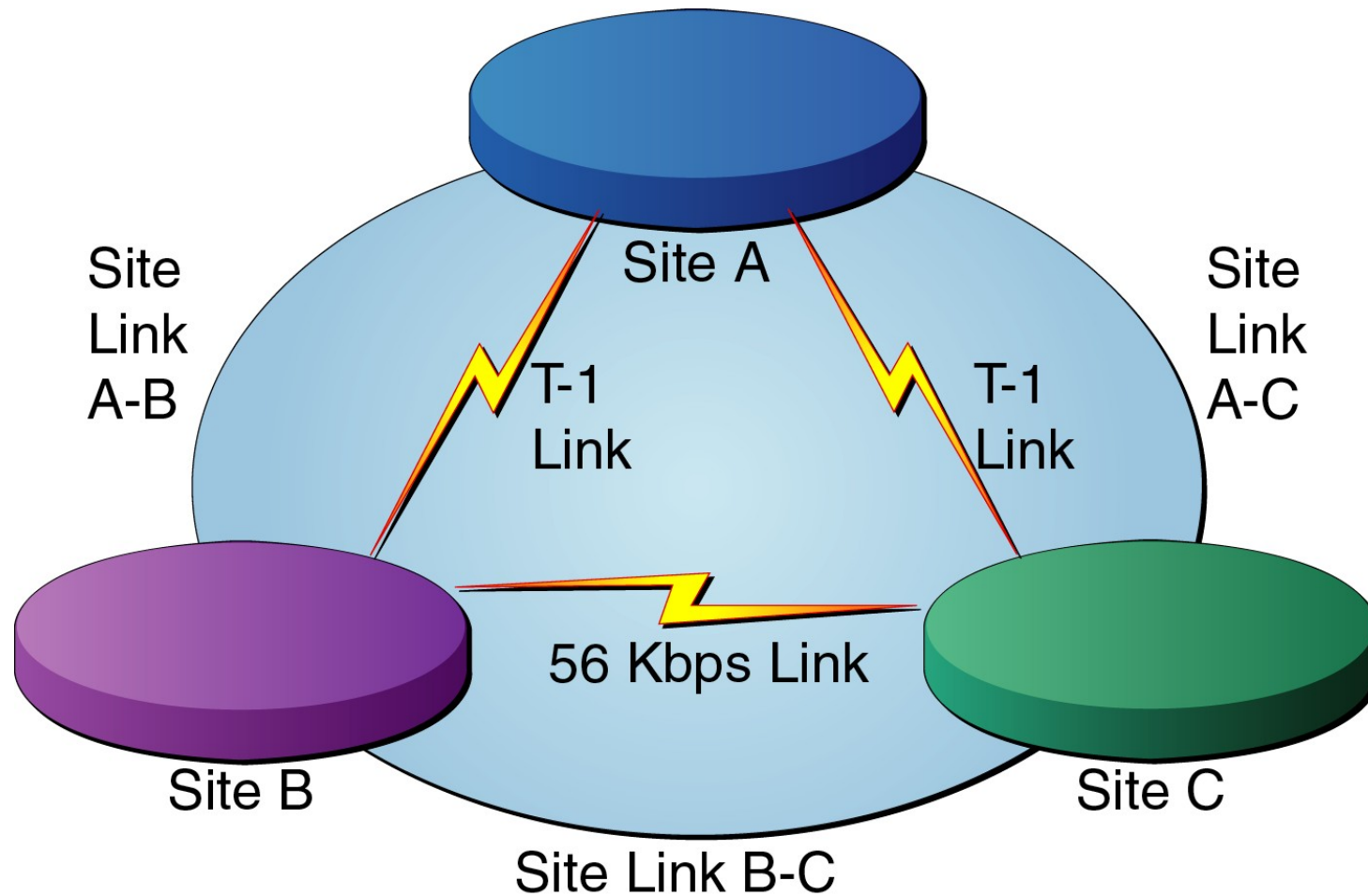
Configuring Site Link Attributes

- When you configure intersite replication, you should provide the following information for all site links:
 - Site link cost
 - Replication frequency
 - Replication availability

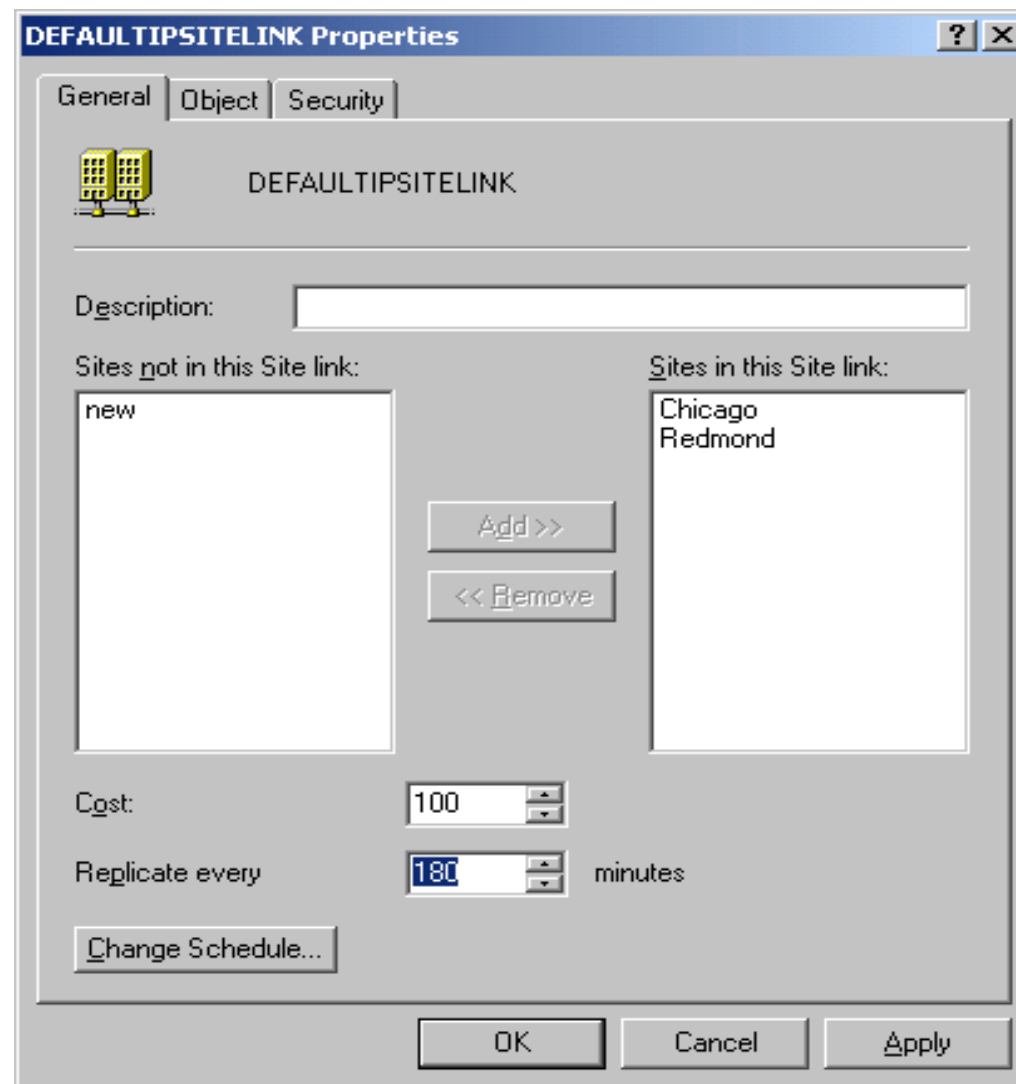
Site Link Cost

- The site link cost assigns a value indicating the relative cost of each available connection used for intersite replication.
- If you have multiple redundant network connections between multiple sites
 - Create a site link object for each connection
 - Then assign a cost to each site link that reflects that link's relative bandwidth
- Cost is a measurement of the priority of each site link.

Example Site Link Configuration



The Properties Dialog Box for a Site Link Object



Replication Frequency

- You configure the replication frequency for site links by specifying how many minutes Active Directory should wait before using a connection to check for replication updates.
 - Default interval = 180 minutes (3 hours)
 - Minimum interval = 15 minutes
 - Maximum interval = 10,080 minutes (1 week)
- You use Active Directory Sites And Services to schedule replication frequency for a site link object.

The Schedule For Dialog Box for a Site Link Object

Schedule for DEFAULTIPSITELINK [X]

12 • 2 • 4 • 6 • 8 • 10 • 12 • 2 • 4 • 6 • 8 • 10 • 12

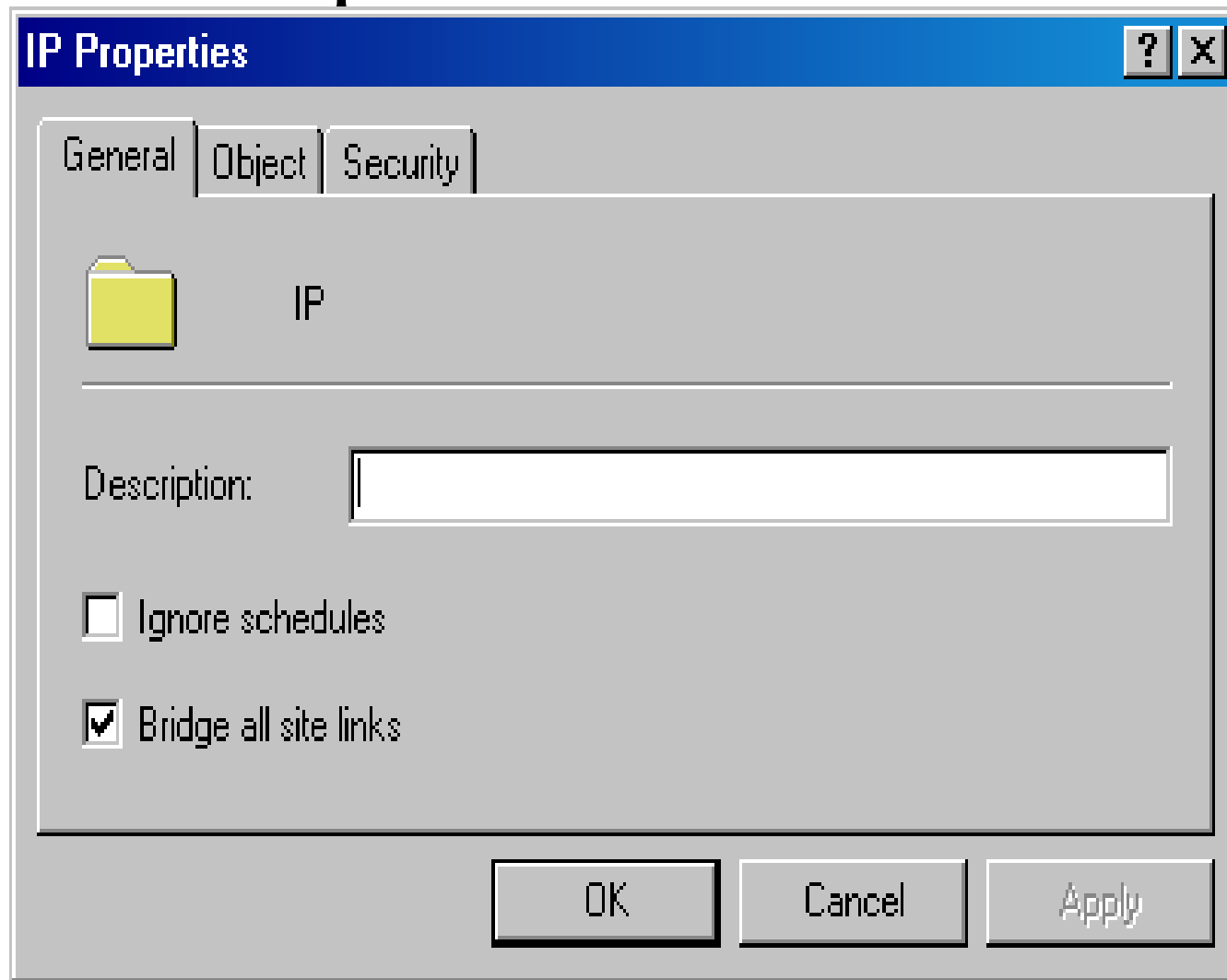
OK
Cancel

All	12	2	4	6	8	10	12	2	4	6	8	10	12
Sunday	■	■	■	■	■	■	■	■	■	■	■	■	■
Monday	■	■	■	■	■	■	■	■	■	■	■	■	■
Tuesday	■	■	■	■	■	■	■	■	■	■	■	■	■
Wednesday	■	■	■	■	■	■	■	■	■	■	■	■	■
Thursday	■	■	■	■	■	■	■	■	■	■	■	■	■
Friday	■	■	■	■	■	■	■	■	■	■	■	■	■
Saturday	■	■	■	■	■	■	■	■	■	■	■	■	■

☐ Replication Not Available
☒ Replication Available

Sunday through Saturday from 12 AM to 12 AM

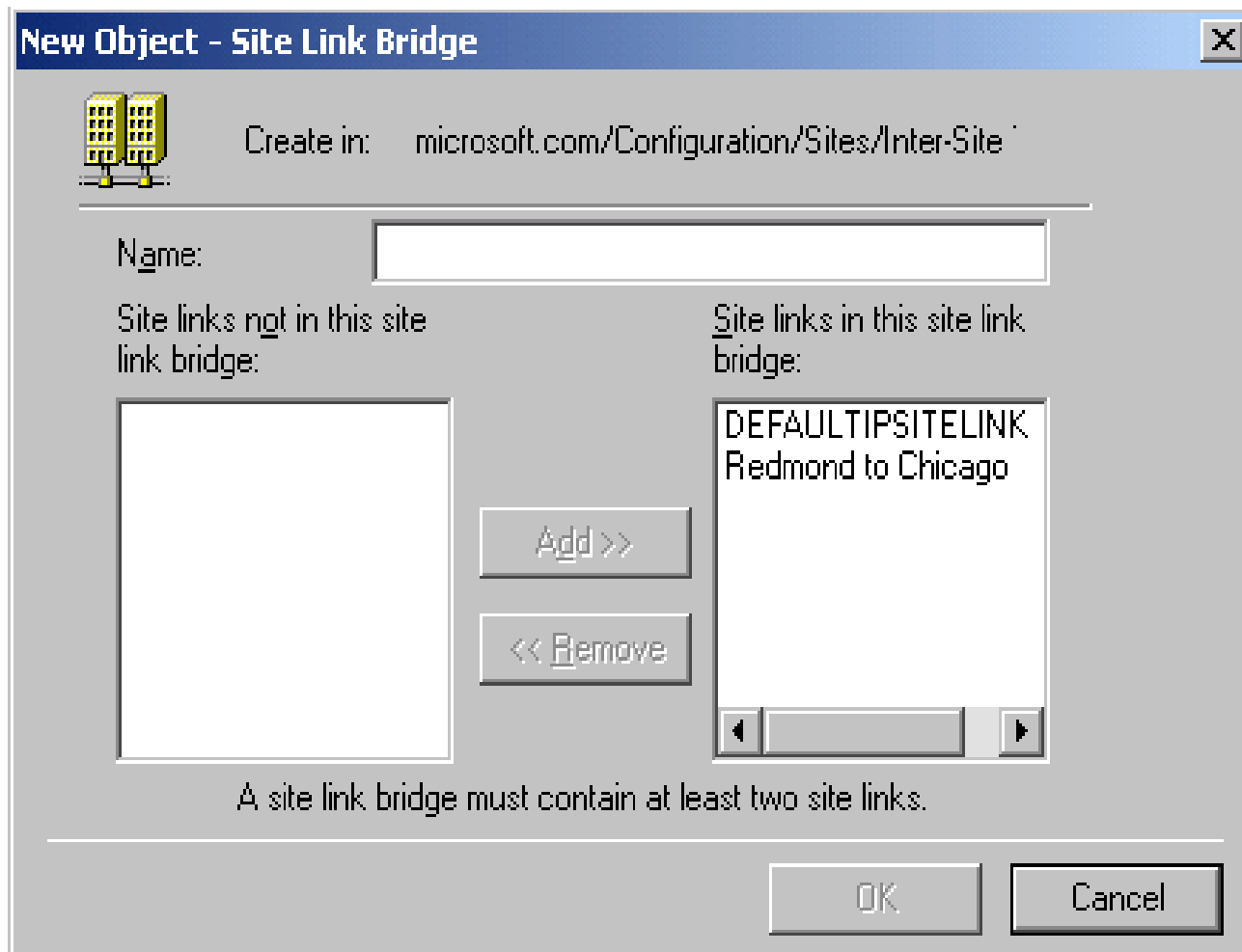
The Properties Dialog Box for an Intersite Transports Protocol Folder



Creating Site Link Bridges

- By default, when more than two sites are linked for replication and they all use the same transport, the site links are *bridged* and *transitive*.
- If your IP network is not fully routed, you can turn off the transitive site link feature for the IP transport and configure site link bridges instead.
- You use Active Directory Sites And Services to create a site link bridge.

The New Object – Site Link Bridge Dialog Box



Operation Master

Schema Master - controls originating updates to the Schema. One domain controller per forest holds this role.

Domain Naming Master - controls the addition / deletion of domains from the forest. This system must also be a Global Catalog Server. One domain controller per forest holds this role.

PDC Emulator - acts as the PDC for BDCs when the domain is in mixed mode, manages password changes for downlevel (pre-win2k) clients, is the focus for group policy changes, and is immediately forwarded all password changes. One domain controller per domain holds this role.

RID Master - allocates the pool of relative identifiers (RIDs, which are the unique part of SIDs) to each domain controller in the domain. One domain controller per domain holds this role. Note that you can view the RID pool allocation using a utility called dcdiag, the domain controller diagnostic utility.

Infrastructure Master - is responsible for updating user-to-group references between domains. This role should not be held on a domain controller which is also acting as a global catalog server - the infrastructure master will not function in this scenario because it holds a copy of all objects, and therefore has no external references. One domain controller per domain holds this role.

When to Transfer Roles

- Initial setup of domain
 - E.g. in a multi-domain forest, move Infrastructure master off global catalog server
- Permanently demoting a DC
 - Roles held by the DC transferred automatically but manual transfer gives control over location
- Temporarily taking down a DC
 - Probably unnecessary to transfer schema and domain naming masters (little used); also infrastructure master in single-domain forest
 - Always transfer the PDC emulator; may be wise to transfer RID master, but probably unnecessary for short downtime

When to Seizing Roles

- Generally only seize when originally role holder has failed irrecoverably and will not be restored from backup
 - Exception — can fairly safely seize PDC emulator role
 - Strangely, this is also the role that you can least do without

Step by Step to Transfer Operation Roles

- In the console tree, right-click Active Directory Users And Computers. Then select Operations Masters.
- For example : The RID tab shows the location of the current relative ID master. Click Change, and then select a new domain controller to transfer the role to a new location.
- The PDC tab shows the location of the current PDC emulator master. Click Change and then select a new domain controller to transfer the role to a new location.
- The Infrastructure tab shows the location of the current infrastructure master. Click Change, and then select a new domain controller to transfer the role to a new location. Click OK.



Configuring Global Catlog Server



Seizing the Operation Master

:

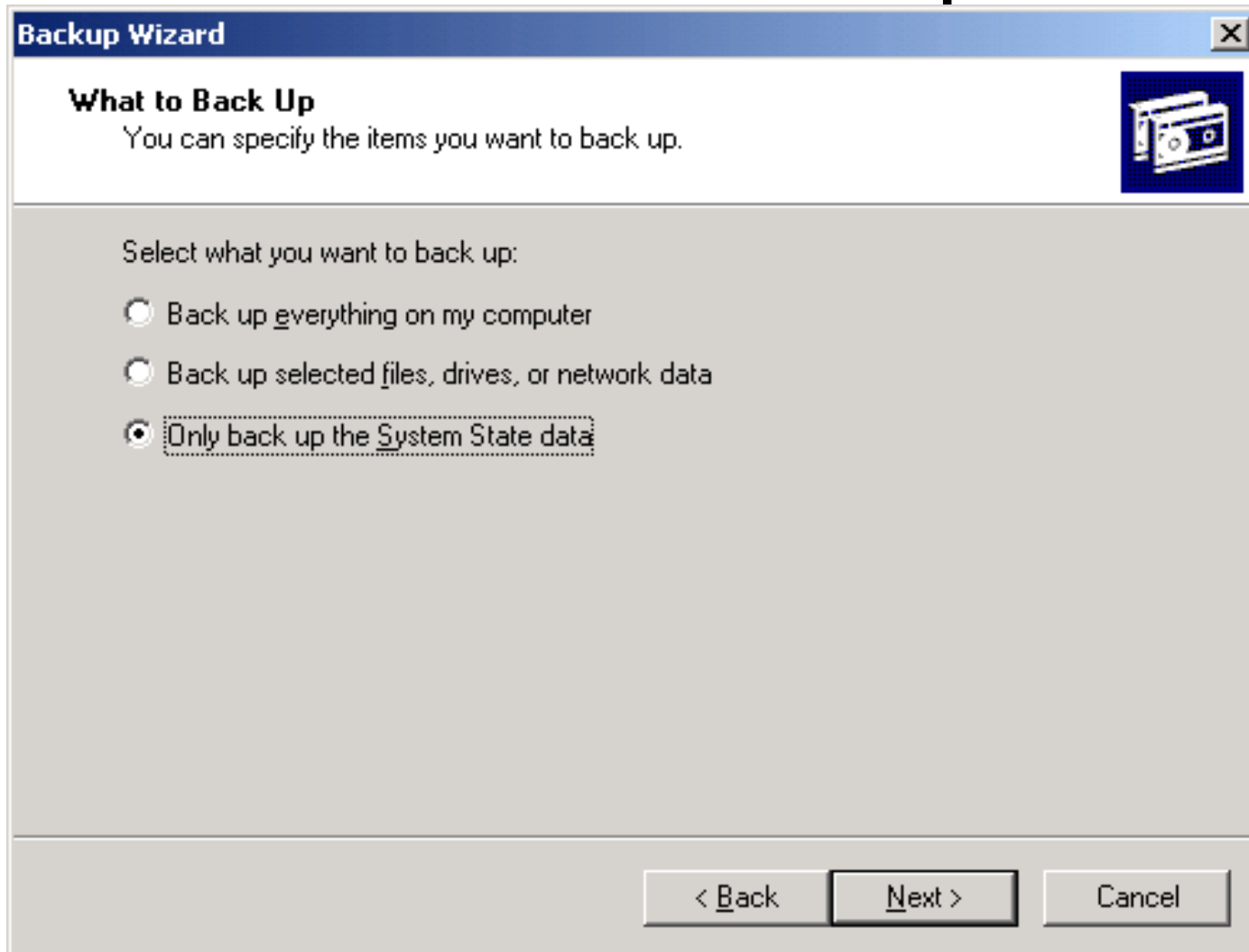
1. Click Start
2. Choose Run
3. Type NTDSUTIL and press Enter
4. At ntdsutil prompt type roles
5. At fsmo maintenance prompt type connections
6. At server connections prompt type connect to server followed by the Fully Qualified Domain Name (FQDN) of the DC that you want to be the new PDC Emulator
7. At server connections prompt type quit
8. At fsmo maintenance prompt type seize PDC
9. At ntdsutil prompt type quit

Backing Up Active Directory

- The Backup Wizard
- What to Back Up
- Where to Store the Backup
- Specifying Advanced Backup Settings
- Scheduling Active Directory Backup Jobs

Backup Wizard

What To Back Up



Backup Wizard

What to Back Up
You can specify the items you want to back up.

Select what you want to back up:

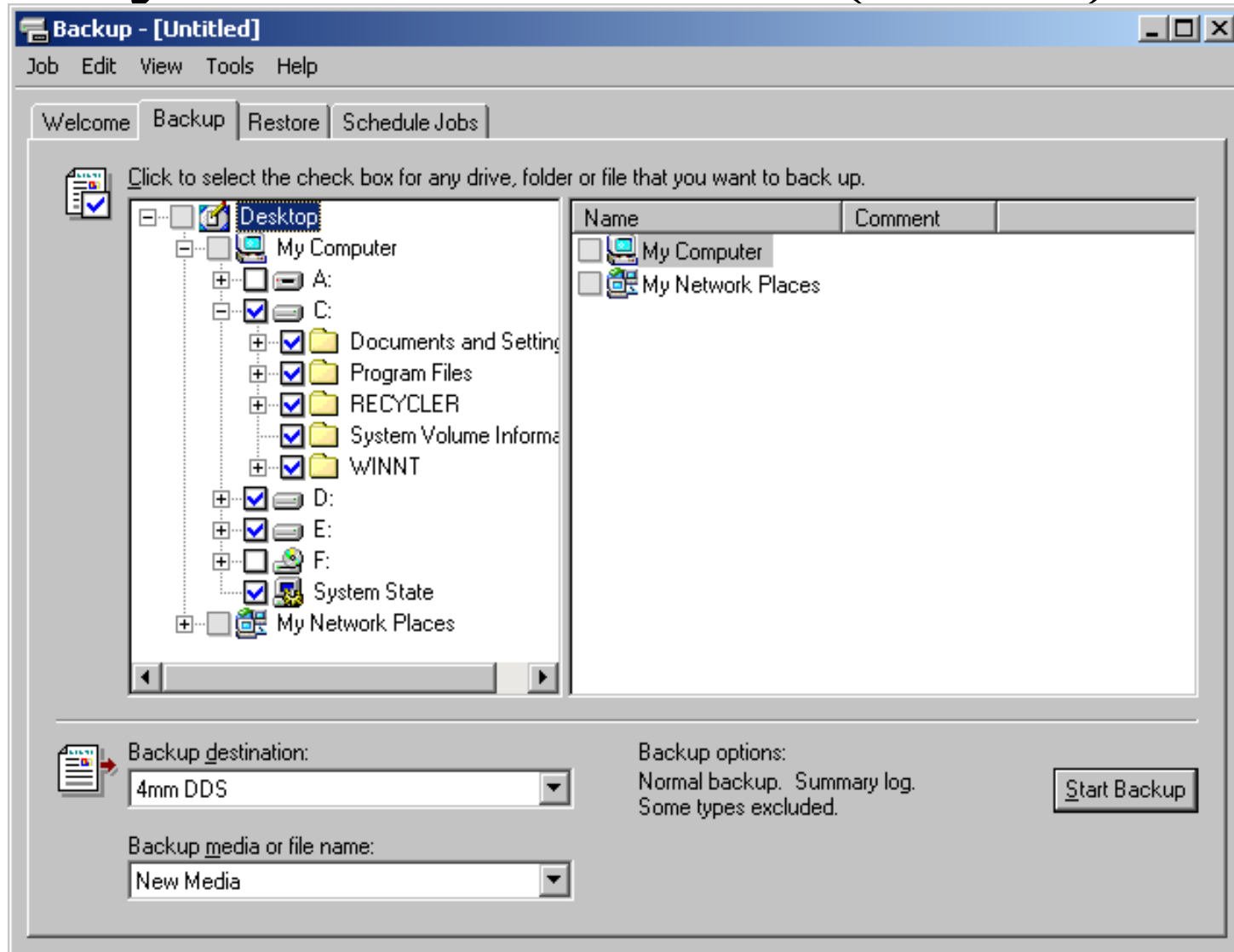
- ☐ Back up everything on my computer
- ☐ Back up selected files, drives, or network data
- ☒ Only back up the System State data

< Back Next > Cancel

Backing Up System State Data

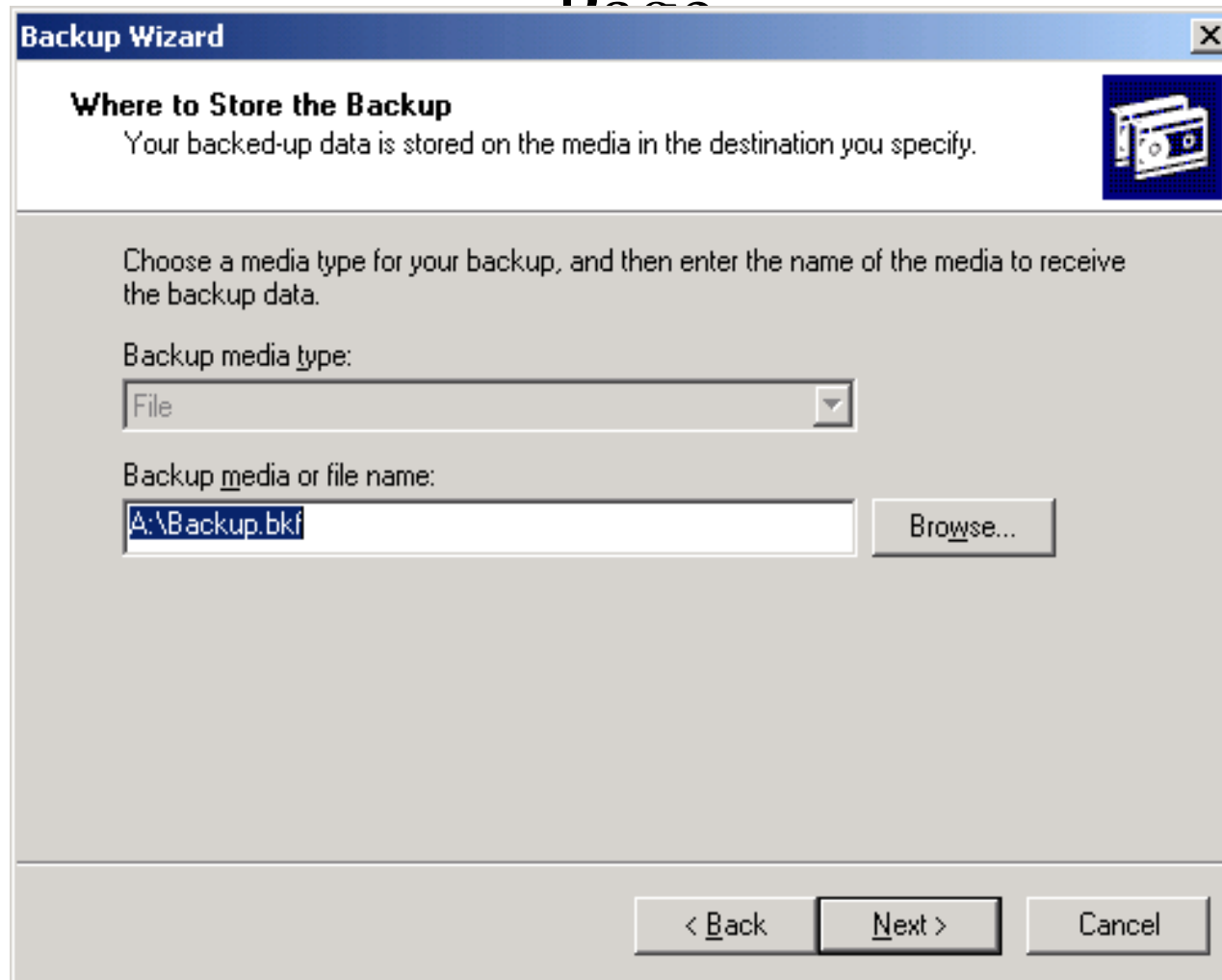
- System State data comprises the registry, the COM+ Class Registration database, system boot files, and the Certificate Services database.
- If the server is a domain controller, Active Directory and the SYSVOL directory are also contained in the System State data.
- All System State data relevant to the computer is backed up; individual components of the System State data cannot be chosen for backup.
- System State data can be backed up on a local computer only; it cannot be backed up on a remote computer.

Backing Up System State Data (Cont.)



Backup Wizard

Where To Store The Backup



The screenshot shows a Windows-style dialog box titled "Backup Wizard". The main heading is "Where to Store the Backup", followed by the instruction "Your backed-up data is stored on the media in the destination you specify." and a small icon of a tape drive. The dialog prompts the user to "Choose a media type for your backup, and then enter the name of the media to receive the backup data." It features a "Backup media type:" label above a dropdown menu currently set to "File". Below this is a "Backup media or file name:" label above a text input field containing "A:\Backup.bkf". To the right of the text field is a "Browse..." button. At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

Backup Wizard

Where to Store the Backup
Your backed-up data is stored on the media in the destination you specify.

Choose a media type for your backup, and then enter the name of the media to receive the backup data.

Backup media type:
File

Backup media or file name:
A:\Backup.bkf

Browse...

< Back Next > Cancel

Backup Media Options

- Backup Media Type
 - Tape or file.
 - File can be located on any disk-based medium, including a hard disk, shared folder, or removable disk.
- Backup Media Or File Name
 - Location where Windows Backup will store the data.
 - For a tape, enter the tape name.
 - For a file, enter the path for the backup file.

Backup Wizard Options

- Start the backup: If Finish is clicked, the Backup Wizard displays status information about the backup job in the Backup Progress dialog box.
- Specify advanced backup options: If Advanced is clicked, the Backup Wizard offers advanced backup settings.

Advanced Backup Settings Pages

- Type Of Backup
- How To Backup
- Media Options
- Backup Label
- When To Back Up

Backup Wizard Provides the Opportunity to do Either of the Following

- Finish the backup process
 - The Backup Wizard displays the Completing The Backup Wizard settings and then presents the option to finish and immediately start the backup.
 - During backup, the wizard displays status information about the backup job.
- Back up later
 - Additional dialog boxes are shown to schedule the backup process to occur later.

Scheduling Active Directory Backup Jobs

- An unattended backup job can occur later when users are not at work and files are closed.
- Active Directory backup jobs should be scheduled to occur at regular intervals.
- Windows 2000 integrates Windows Backup with the Task Scheduler service.

Preparing to Restore Active Directory

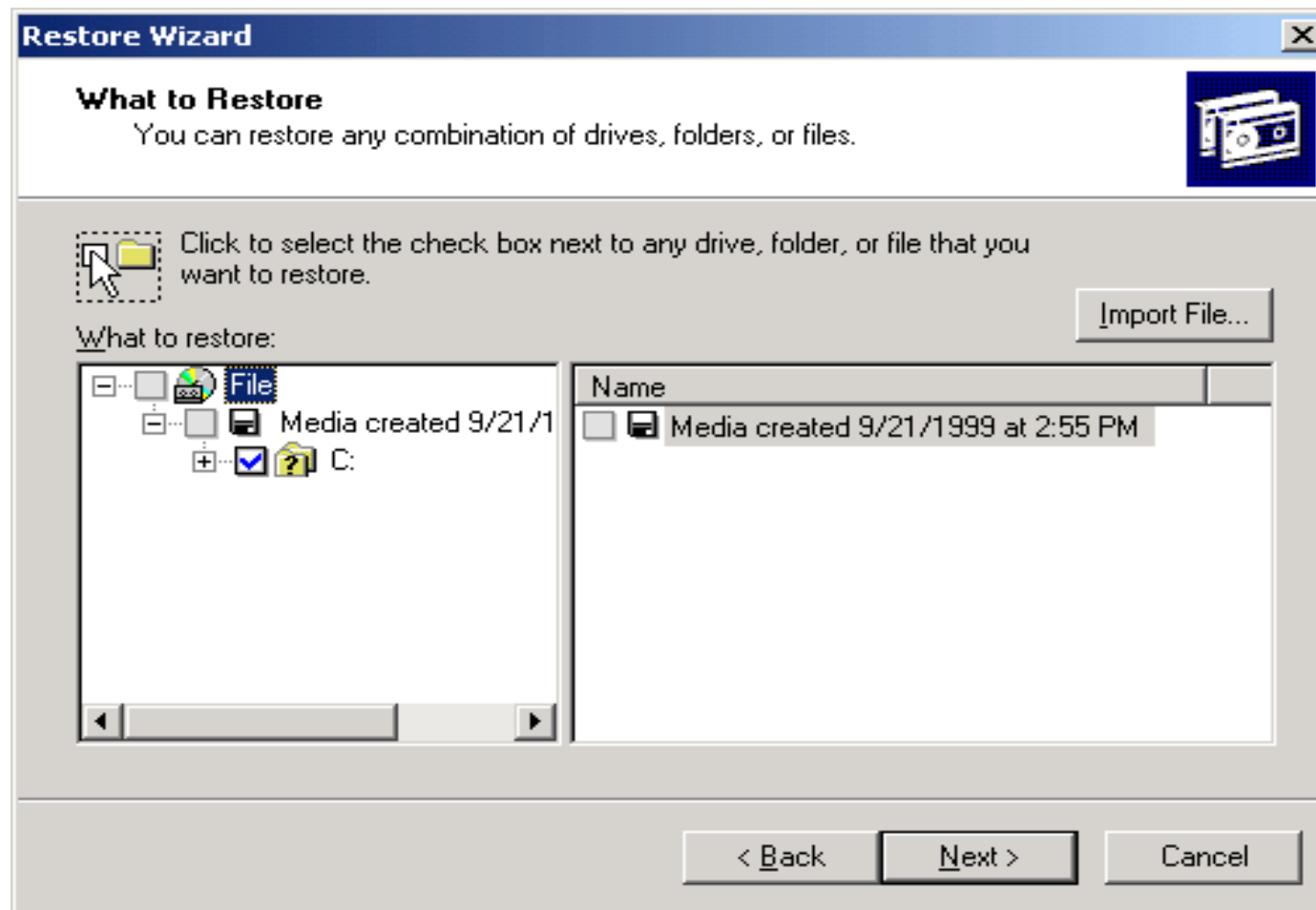
- As with the backup process, only the System State data that was backed up can be restored, including the registry, the COM+ Class Registration database, system boot files, the SYSVOL directory, the Active Directory, and the Certificate Services database.
- Individual components of the System State data cannot be restored.
- If the System State data is being restored to a domain controller, the choice of whether to perform a nonauthoritative restore or an authoritative restore must be specified.
- Default method of restoring the System State data to a domain controller is nonauthoritative.

Nonauthoritative Restore

- Any component of the System State replicated with another domain controller is brought up-to-date by replication after the data is restored.
- The Active Directory replication system updates the restored data with newer data from other servers.

Restore Wizard

What To Restore Page



Restore Wizard:

Advanced Restore Options

- Where To Restore page: Restore Files To option
- How To Restore page: When Restoring Files That Already Exist option
- Advanced Restore Options page: Select The Special Restore Options You Want To Use option

Windows Backup Functions After the Restore Wizard

- Prompts for verification of the selection of the source media to use to restore data; after verification, Windows Backup starts the restore process.
- Displays status information about the restore process.

Performing an Authoritative Restore:

Authoritative Restore Operation

- An authoritative restore occurs after a nonauthoritative restore and designates the entire directory, a subtree, or individual objects to be recognized as authoritative with respect to replica domain controllers in the forest.
- The NTDSUTIL utility allows objects to be marked as authoritative so that they are propagated through replication, thereby updating existing copies of those objects throughout the forest.

Performing an Authoritative Restore: After the Authoritative Restore Operation

- Normal replication brings the restored domain controller up-to-date with any changes from the additional domain controllers that were not overridden by the authoritative restore.
- Replication also propagates the authoritatively restored object(s) to other domain controllers in the forest.
- The deleted objects that were marked as authoritative are replicated from the restored domain controller to the additional domain controllers.
- Because the restored objects have the same object GUID and object SID, security remains intact, and object dependencies are maintained.

Additional Tasks for Authoritatively Restoring the Entire Active Directory Database

- An additional procedure involving the SYSVOL directory must be performed to ensure the integrity of the computer's group policy.
- Which additional procedure should be performed depends on whether the entire Active Directory database or only a portion is being authoritatively restored.

Active Directory Performance Monitoring Tools

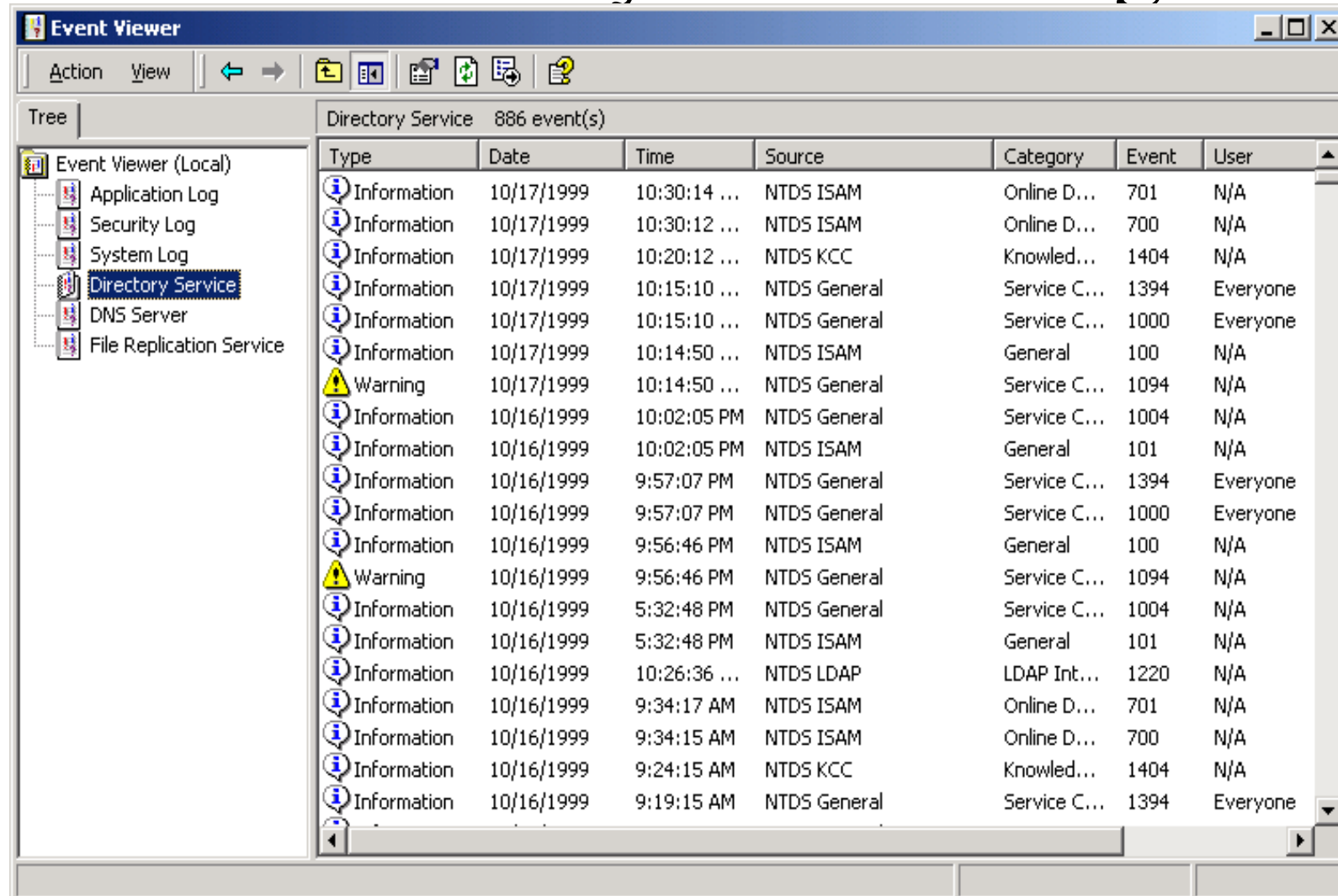
- Performance Monitoring Tools
- The Event Viewer Console
- The Performance Console
- System Monitor
- Performance Logs and Alerts

Uses for Active Directory Performance Data

- Understand Active Directory performance and the corresponding effect on the system's resources
- Observe changes and trends in performance and resource usage to enable future planning
- Test configuration changes or other tuning efforts by monitoring the results
- Diagnose problems and target components or processes for optimization

Event Viewer Console

Directory Service Log



Event Viewer

Tree

- Event Viewer (Local)
 - Application Log
 - Security Log
 - System Log
 - Directory Service
 - DNS Server
 - File Replication Service

Directory Service 886 event(s)

Type	Date	Time	Source	Category	Event	User
Information	10/17/1999	10:30:14 ...	NTDS ISAM	Online D...	701	N/A
Information	10/17/1999	10:30:12 ...	NTDS ISAM	Online D...	700	N/A
Information	10/17/1999	10:20:12 ...	NTDS KCC	Knowled...	1404	N/A
Information	10/17/1999	10:15:10 ...	NTDS General	Service C...	1394	Everyone
Information	10/17/1999	10:15:10 ...	NTDS General	Service C...	1000	Everyone
Information	10/17/1999	10:14:50 ...	NTDS ISAM	General	100	N/A
Warning	10/17/1999	10:14:50 ...	NTDS General	Service C...	1094	N/A
Information	10/16/1999	10:02:05 PM	NTDS General	Service C...	1004	N/A
Information	10/16/1999	10:02:05 PM	NTDS ISAM	General	101	N/A
Information	10/16/1999	9:57:07 PM	NTDS General	Service C...	1394	Everyone
Information	10/16/1999	9:57:07 PM	NTDS General	Service C...	1000	Everyone
Information	10/16/1999	9:56:46 PM	NTDS ISAM	General	100	N/A
Warning	10/16/1999	9:56:46 PM	NTDS General	Service C...	1094	N/A
Information	10/16/1999	5:32:48 PM	NTDS General	Service C...	1004	N/A
Information	10/16/1999	5:32:48 PM	NTDS ISAM	General	101	N/A
Information	10/16/1999	10:26:36 ...	NTDS LDAP	LDAP Int...	1220	N/A
Information	10/16/1999	9:34:17 AM	NTDS ISAM	Online D...	701	N/A
Information	10/16/1999	9:34:15 AM	NTDS ISAM	Online D...	700	N/A
Information	10/16/1999	9:24:15 AM	NTDS KCC	Knowled...	1404	N/A
Information	10/16/1999	9:19:15 AM	NTDS General	Service C...	1394	Everyone

Event Logs for Monitoring Active Directory Performance

- Application log: Contains errors, warnings, or information that applications, such as a database server or an e-mail program, generate
- Directory Service log: Contains errors, warnings, and information that Active Directory generates
- File Replication Service log: Contains errors, warnings, and information that the File Replication service generates
- System log: Contains errors, warnings, and information that Windows 2000 generates

NTDS Performance Object Counters

- The NTDS performance object contains many performance counters that provide statistics about Active Directory performance.
- After determining the desired statistics to monitor, the matching performance counters must be found.
- Performance counters can provide some baseline analysis information for capacity and performance planning.
- Counters that are suited for capacity planning contain the word “total” in their name.
- Each counter has its own guidelines and limits.

Trace Log–Specific Options in the Log Files Tab

- Log File Type: The desired format for this log file
 - Circular Trace File: Defines a circular trace log file (.etl), used to record data continuously to the same log file, overwriting previous records with new data.
 - Sequential Trace File: Defines a sequential trace log file (.etl) that collects data until it reaches a user-defined limit and then closes and starts a new file.
- Log File Size: Select this option for circular logging
 - Maximum Limit: Data is continuously collected in a log file until it reaches limits set by disk quotas or the OS.
 - Limit Of: The maximum size, in megabytes, of the log file.

Active Directory Support Tools

- LDP.EXE: Active Directory Administration Tool
- REPLMON.EXE: Active Directory Replication Monitor
- REPADMIN.EXE: Replication Diagnostics Tool
- DSASTAT.EXE: Active Directory Diagnostic Tool
- SDCHECK.EXE: Security Descriptor Check Utility
- NLTEST.EXE
- ACLDIAG.EXE: ACL Diagnostics
- DSACLS.EXE

GUI Tools

- **LDP.EXE:** Active Directory Administration Tool
- Allows users to perform LDAP operations, such as connect, bind, search, modify, add, and delete, against any LDAP-compatible directory
 - LDAP is an Internet standard wire protocol used by Active Directory.
- Graphical tool located on the Tools menu within Windows 2000 Support Tools
- Used by administrators to view objects stored in Active Directory along with their metadata, such as security descriptors and replication metadata

GUI Tools

- **REPLMON.EXE:** Active Directory Replication Monitor
- Enables administrators to do various tasks
 - View the low-level status of Active Directory replication
 - Force synchronization between domain controllers
 - View the topology in a graphical format
 - Monitor the status and performance of domain controller replication through a graphical interface
- Located on the Tools menu within Windows 2000 Support Tools

Active Directory Replication Monitor Features

- Graphic displays
- Replication status history
- Property pages
- Status report generation
- Server Wizard
- Graphical site topology
- Properties display
- Statistics and replication state polling
- Replication triggering
- KCC triggering
- Display nonreplicated changes

REPADMIN.EXE: Replication Diagnostic Tool

- Command-line tool that assists administrators in diagnosing replication problems between Windows 2000 domain controllers
- Allows the administrator to view the replication topology as seen from the perspective of each domain controller
- Used to manually create the replication topology, force replication events between domain controllers, and view both the replication metadata and up-to-dateness vectors

DSASTAT.EXE: Active Directory Diagnostic Tool

- Command-line tool that compares and detects differences between naming contexts on domain controllers
- Used to compare two directory trees across replicas within the same domain or, in the case of a global catalog, across different domains
- Retrieves capacity statistics, such as MB per server, objects per server, ~~Confidential~~ MB per object class, and performs comparisons of attributes of replicated object

SDCHECK.EXE: Security Descriptor Check Utility

- Command-line tool that displays the security descriptor for any object stored in the Active Directory
- Displays the object hierarchy and any ACLs that are inherited by the object from its parent
- Displays the security descriptor propagation metadata so that administrators can monitor these changes with respect to propagation of inherited ACLs as well as replication of ACLs from other domain controllers
- Used to ensure that domain controllers are up-to-date with one another

NLTEST.EXE

- Command-line tool that helps perform network administrative tasks
 - Test trust relationships and the state of a domain controller replication in a Windows domain
 - Query and check on the status of trust
 - Force a shutdown
 - Get a list of PDCs
 - Force a user account database into sync on Windows NT 4.0 or earlier domain controllers
- Runs only on x86-based machines

ACL Diagnostics: ACLDIAG.EXE

- Command-line tool that helps diagnose and troubleshoot problems with permissions on Active Directory objects
- Reads security attributes from ACLs and outputs information in either readable or tab-delimited format
 - Tab-delimited format can be uploaded into a text file for searches on particular permissions, users, or groups, or into a spreadsheet or database for reporting.
- Provides some simple cleanup functionality
- Displays only the permissions of objects the user has the right to view
- Can't be used on GPOs because they are virtual objects that have no distinguished name

DSACLS.EXE

- Command-line tool that facilitates management of ACLs for directory services
- Used for general-purpose ACL reporting and setting from the command prompt
- Enables administrators to query and manipulate security attributes on Active Directory objects
- Command-line equivalent of the Security page on various Active Directory snap-in tools
- Provides security configuration and diagnosis functionality on Active Directory objects

Troubleshooting Active Directory

- Cannot add/remove a domain
- Cannot create objects
- Cannot modify the schema
- Changes to group membership not taking effect
- Clients without Active Directory client software cannot log on
- Unable to access resources in another domain

Symptom: Cannot Add/Remove a Domain

- Cause:
 - Domain naming master is not available.
 - Network connectivity problem
 - Failure of computer holding the domain naming master role
- Solution:
 - Resolve the network connectivity problem.
 - Repair/replace domain naming master computer.

Symptom: Cannot Create Objects in Active Directory

- Cause:
 - Relative ID master is not available.
 - Network connectivity problem
 - Failure of computer holding the relative ID master role
- Solution:
 - Resolve network connectivity problem.
 - Repair/replace relative ID master computer.

Symptom: Cannot Modify the Schema

- Cause:
 - Schema master is not available.
 - Network connectivity problem
 - Failure of computer holding the schema master role
- Solution:
 - Resolve network connectivity problem.
 - Repair/replace schema master computer.

Symptom: Changes to Group Memberships Not Taking Effect

- Cause:
 - Infrastructure master is not available.
 - Connectivity problem
 - Failure of computer holding the infrastructure master role
- Solution:
 - Resolve network connectivity problem.
 - Repair/replace infrastructure master computer.

Symptom: Clients Without Active Directory Client Software Installed Cannot Log On

- Cause:
 - Primary domain controller emulator is not available.
 - Network connectivity problem
 - Failure of computer holding the primary domain controller emulator role
- Solution:
 - Resolve network connectivity problem.
 - Repair/replace primary domain controller emulator computer.

Symptom: Unable to Access Resources in Another Domain

- Cause:
 - Failure of the trust between the domains.
- Solution:
 - Reset and verify the trust between domains.
 - The PDC emulator must be available to reset trust.

Troubleshooting Active Directory Replication

- Most Active Directory replication problems that can be fixed with Active Directory Sites And Services involve poor directory information.

Replication Problems

- Ineffective replication can result in poor Active Directory performance and network problems, such as new users not being recognized.
- Replication problems usually result in out-of-date Active Directory information or unavailable domain controllers.

Replication Troubleshooting Scenarios

- Symptom: Replication of directory information has stopped.
 - Cause: The sites containing the clients and domain controllers are not connected by site links to domain controllers in other sites on the network.
 - Solution: Create a site link object joining the current site to a site that is connected to the rest of the network's sites.
- Symptom: Replication has slowed but not stopped.
 - Possible cause #1: The intersite replication structure is not as complete as it should be.
 - Possible solution #1: Make sure Active Directory is configured properly. Consider creating a site link bridge or bridging all of the site links.

Replication Troubleshooting Scenarios (Cont.)

- Symptom: Replication has slowed but not stopped. (Cont.)
 - Possible cause #2: Current network resources are insufficient to handle the amount of replication traffic.
 - Possible solution #2: There are several possible solutions:
 - Increase available network resources for directory traffic.
 - Decrease the frequency of replication.
 - Configure site link costs.
 - Create site links or site link bridges.
- Symptom: Replication has slowed but not stopped. (Cont.)
 - Possible cause #3: Directory information that is changed on domain controllers at one site is not being updated on domain controllers at other sites in a timely manner because intersite replication is scheduled too infrequently.
 - Possible solution #3: Increase the frequency of replication, and if a site link is restricting replication, increase the time range during which replication can occur on that site link.

Replication Troubleshooting Scenarios (Cont.)

- Symptom: Replication has slowed but not stopped. (Cont.)
 - Possible cause #4: Clients are requesting services from a domain controller with a low-bandwidth connection.
 - Possible solution #4: There are several possible solutions:
 - Check for a site that better serves the client's subnet.
 - If a client is isolated from domain controllers, consider creating another site with its own domain controller that includes the client.
 - Install a connection with more bandwidth.