

Module 11: Managing Active Directory Replication

Contents

Overview	1
Introduction to Active Directory Replication	2
Replication Components and Processes	3
Replication Topology	9
Lab A: Tracking Active Directory Replication	15
Using Sites to Optimize Active Directory Replication	22
Implementing Sites to Manage Active Directory Replication	28
Lab B: Using Sites to Manage Active Directory Replication	35
Monitoring Replication Traffic	40
Adjusting Replication	44
Lab C: Monitoring Replication	46
Troubleshooting Active Directory Replication	50
Best Practices	52
Review	53



Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, places or events is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, BackOffice, FrontPage, IntelliMirror, PowerPoint, Visual Basic, Visual Studio, Win32, Windows, Windows Media, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Instructor Notes

Presentation:
105 Minutes

This module provides students with the knowledge and skills to manage Active Directory® directory service replication within a site and between sites.

Labs:
60 Minutes

At the end of this module, students will be able to:

- Identify the importance of replication in a Microsoft® Windows® 2000 network.
- Describe the components of replication and the replication process.
- Describe how the replication topology enables and optimizes replication throughout a network.
- Describe how sites enable you to optimize Active Directory replication.
- Use sites to manage Active Directory replication.
- Monitor replication traffic.
- Adjust the replication behavior to improve replication performance.
- Troubleshoot common problems with Active Directory replication.
- Apply best practices for managing Active Directory replication.

In the hands-on labs in this module, students will have the opportunity to manage Active Directory replication. In the first lab, students will track Active Directory replication. In the second lab, students will create sites, subnets, and site links to manage replication. In the third lab, students will monitor the replication traffic.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the following materials:

- Microsoft PowerPoint® file 2154A_11.ppt

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the labs.
- Study the review questions and prepare alternative answers to discuss.
- Anticipate questions that students may ask. Write out the questions and provide the answers.
- Read chapter 6, “Active Directory Replication” in the Distributed Systems book in the Microsoft Windows 2000 Server Resource Kit.

Module Strategy

Use the following strategy to present this module:

- **Introduction to Active Directory Replication**

In this topic, you will introduce the role of replication in improving the performance of Active Directory in a Windows 2000 network. Explain the importance of replication in a Windows 2000 network.

- **Replication Components and Processes**

In this topic, you will introduce the components of replication and the replication process. Discuss the reasons why replication occurs, and the two types of replication updates. Emphasize the differences between originating and replicated updates. Present the concept of replication latency during normal and urgent replication. Emphasize the change notification process. Use the slide in the Replication Latency topic to describe normal and urgent replication. Next, discuss why conflicts occur during replication, and how conflicts are resolved during replication. Finally, explain how propagation dampening enables optimizing replication.

- **Replication Topology**

In this topic, you will introduce the replication topology. Explain how the directory partitions enable replication among the domain controllers during replication. Discuss the purpose of replication topology. The slide for this topic is animated. The first slide illustrates replication topology in a single domain; the second slide illustrates replication topology in multiple domains. Use the animated slides to illustrate how replication topology is modified when a new global catalog server is added to the forest. Explain how KCC enables automatic replication topology generation by using the animated slide. Illustrate the role of connection objects in replication.

- **Lab A: Tracking Active Directory Replication**

Prepare students for the lab in which they will identify the results of attribute, sibling name, and add/move under deleted container replication conflicts. Students will also initiate replication of updates by using the connection objects for direct replication partners. After students have completed the lab, ask them if they have any questions concerning the lab.

- **Using Sites to Optimize Active Directory Replication**

In this topic, you will introduce how to use sites to optimize Active Directory replication. Discuss what sites are. Have students participate in this discussion because they should already know about sites. Discuss how replication occurs within sites and between sites. Explain how replication transports provide the protocols required for data transfer.

- **Implementing Sites to Manage Active Directory Replication**

In this topic, you will introduce how to implement sites to manage Active Directory replication. Demonstrate how to create sites and subnets, create and configure site links, and create site link bridges. Briefly explain the naming rules for defining sites. Point out to the students the site links that are created in Active Directory Sites and Services. Emphasize that multiple site link bridges work independently of one another.

- Lab B: Using Sites to Manage Active Directory Replication

Prepare students for the lab in which they will create a site, subnet, site link, and site link bridge, and then configure site link properties. After students have completed the lab, ask them if they have any questions concerning the lab.

- Monitoring Replication Traffic

In this topic, you will introduce how to monitor replication traffic. Discuss the reasons to monitor replication traffic by using Replication Monitor. Demonstrate how to monitor replication traffic by using Replication Monitor and the **repadmin** utility. Explain the output results of Replication Monitor and the **repadmin** utility.

- Adjusting Replication

In this topic, you will introduce making adjustments to improve replication performance. Demonstrate different types of adjustments that can be made to improve replication performance. Emphasize that Active Directory replication occurs automatically with no administrative intervention. Therefore, administrators should modify a replication topology only if absolutely necessary.

- Lab C: Monitoring Replication

Prepare students for the lab in which they will monitor replication by using Replication Monitor and the **repadmin** utility. After students have completed the lab, ask them if they have any questions concerning the lab.

- Troubleshooting Active Directory Replication

In this topic, you will introduce troubleshooting options for resolving problems that may occur when managing Active Directory replication. Describe some of the more common problems that students may encounter when managing Active Directory replication, along with suggested strategies for resolving these problems.

- Best Practices

Present best practices for managing Active Directory replication. Emphasize the reason for each best practice.

Customization Information

This section identifies the lab setup requirements for the module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The labs in this module are also dependent upon the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.

Lab Setup

The following list describes the setup requirements for the labs in this module.

Setup Requirement 1

The labs in this module require student computers to be configured as domain controllers in child domains of nwtraders.msft. There are two student computers for each child domain. To prepare student computers to meet this requirement, perform one of the following actions:

- Complete the labs in Module 10, “Creating and Managing Trees and Forests,” in Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.
- Run Change.vbs from the C:\Moc\Win2154A\Labfiles\Custom\Autode folder.
- Run Dcpromo.exe on the student computers by using the following parameters:
 - A domain controller for a new domain (first computer only).
 - The existing domain tree, which is nwtraders.msft (first computer only).
 - A domain controller for the existing domain (second computer only).
 - Full DNS domain name, which is *domain.nwtraders.msft* (where *domain* is the assigned domain name).
 - The NetBIOS domain name, which is *DOMAIN*.
 - Default location for the database, log files, and SYSVOL.
 - Permission compatible only with Windows 2000–based servers.
 - Directory Services Restore Mode administrator password, which is **password**.

Setup Requirement 2

The labs in this module require the domain to be in native mode. To prepare student computers to meet this requirement, perform one of the following actions:

- Complete the labs in Module 10, “Creating and Managing Trees and Forests,” in Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.
- Run Nativesd.vbs from the C:\Moc\Win2154a\Labfiles\Custom\Autodc folder.
- Change the domain mode to native in the *domain* (where *domain* is your assigned domain name) **Properties** dialog box in Active Directory Domains and Trusts.

Lab Results

Performing the labs in this module introduces the following configuration changes:

- An Internet Protocol (IP) Subnet object 10.10.*n*.0 (where *n* is the assigned student number) is created for each student computer.
- A site *servername*Site (where *servername* is the host name of their computer) is created for each student computer.
- A site link *servername*Site –CorpHQ is created for each student computer.
- A site link bridge *servername*Site –CorpHQ–Bridge is created for each student computer.
- Windows 2000 Support Tools are installed.

Overview

Topic Objective

To provide an overview of the module topics and objectives.

Lead-in

In this module, you will learn about managing Active Directory replication within a site and between sites.

- Introduction to Active Directory Replication
- Replication Components and Processes
- Replication Topology
- Using Sites to Optimize Active Directory Replication
- Implementing Sites to Manage Active Directory Replication
- Monitoring Replication Traffic
- Adjusting Replication
- Troubleshooting Active Directory Replication
- Best Practices

*****ILLEGAL FOR NON-TRAINER USE*****

Microsoft® Windows® 2000 Active Directory® directory service replication involves transferring and maintaining Active Directory data between domain controllers in a network. Active Directory uses a *multi-master replication model*. Multi-master means that there are multiple domain controllers, otherwise called masters, which have the authority to modify or control the same information. So the replication model must copy or replicate the data changed on one domain controller to another. The multi-master model must address the fact that changes can be made by more than one domain controller. By understanding how Active Directory replication is managed, you can control replication network traffic and ensure the consistency of Active Directory data across your network.

At the end of this module, you will be able to:

- Identify the importance of replication in a Windows 2000 network.
- Describe the components of replication and the replication process.
- Describe how replication topology enables and optimizes replication throughout a network.
- Describe how sites enable you to optimize Active Directory replication.
- Use sites to manage Active Directory replication.
- Monitor replication traffic.
- Adjust the replication behavior to improve replication performance.
- Troubleshoot common problems with Active Directory replication.
- Apply best practices for managing Active Directory replication.

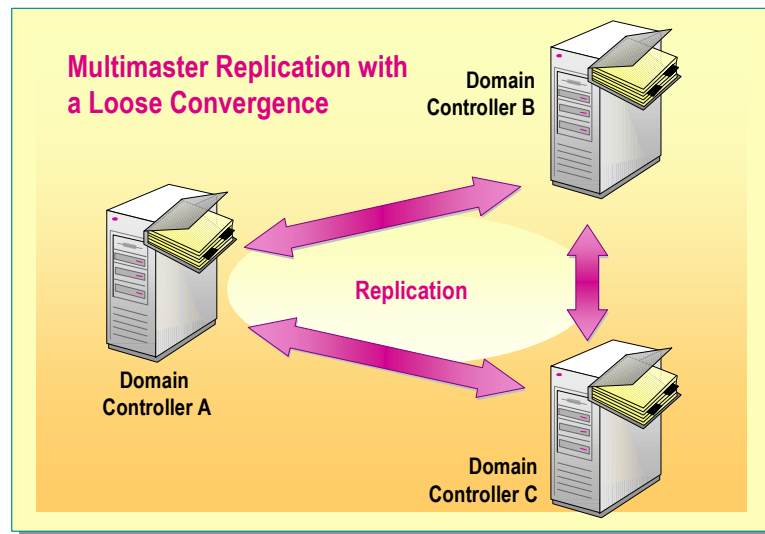
Introduction to Active Directory Replication

Topic Objective

To illustrate the importance of replication in a Windows 2000 network.

Lead-in

Replication ensures that all information in Active Directory is available to all domain controllers and client computers across the entire network.



*****ILLEGAL FOR NON-TRAINER USE*****

Introduce the basic concept of replication without using any technical terms. Tell the students that replication can occur within or between sites. Do not go into the details of how replication occurs in these two situations.

One of the exceptions for the first advantage of multi-master replication is the operations master roles. For information on operation master roles, see Module 12, "Managing Operations Masters," in Course 2154, *Implementing and Administering Microsoft Windows 2000 Directory Services*.

Replication is the process of updating information in Active Directory from one domain controller to the other domain controllers in a network. Replication synchronizes the copying of data on each domain controller. Synchronization ensures that all information in Active Directory is available to all domain controllers and client computers across the entire network.

When a user or administrator performs an action that initiates an update to Active Directory, an appropriate domain controller is automatically chosen to perform the update. This change is made transparently at one of the domain controllers.

Active Directory provides multi-master replication with loose convergence. Multi-master replication provides two advantages for Active Directory:

- With few exceptions, there is no single domain controller that, if unavailable, must be replaced before updates to Active Directory can resume.
- Domain controllers can be distributed across the network and located in multiple physical sites. Locating domain controllers at multiple physical sites enables fault tolerance.

Active Directory uses sites to identify well-connected computers within an organization to optimize network bandwidth. *Replication within sites* occurs between domain controllers in the same site, and is designed to work with fast, reliable connections. *Replication between sites* occurs between the domain controllers located on different sites, and is designed under the assumption that the network links between sites have limited bandwidth and availability.

◆ Replication Components and Processes

Topic Objective

To introduce the topics related to replication components and processes.

Lead-in

In addition to the physical structure, other components influence replication.

- How Replication Works
- Replication Latency
- Resolving Replication Conflicts
- Optimizing Replication

*****ILLEGAL FOR NON-TRAINER USE*****

Replication of updates is initiated when one or more objects on a domain controller are added, modified, deleted, or moved. When one of these updates occurs, the replication process occurs between domain controllers through the interaction of components of replication. Replication in Active Directory propagates changes and tracks the changes among domain controllers. Each domain controller in a forest stores a copy of specific parts of the Active Directory structure. Although replication has the effect of synchronizing information in Active Directory for an entire forest of domain controllers, the actual process of replication occurs between only two domain controllers at a time. Because the domain controllers are both masters for the data and each has its own updatable copy, delay in replication across domain controllers may sometimes result in replication conflicts between domain controllers. Active Directory automatically resolves these conflicts.

Important It is recommended that you secure the channels that Active Directory uses for replication. For more information on Securing Communication channels see Module 7, Securing Communication Channels, in Course 2150, *Designing a Secure Microsoft Windows 2000 Network*.

Or see the Technet article on Active Directory Replication over Firewalls at <http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/ittasks/tasks/adrepfir.asp>.

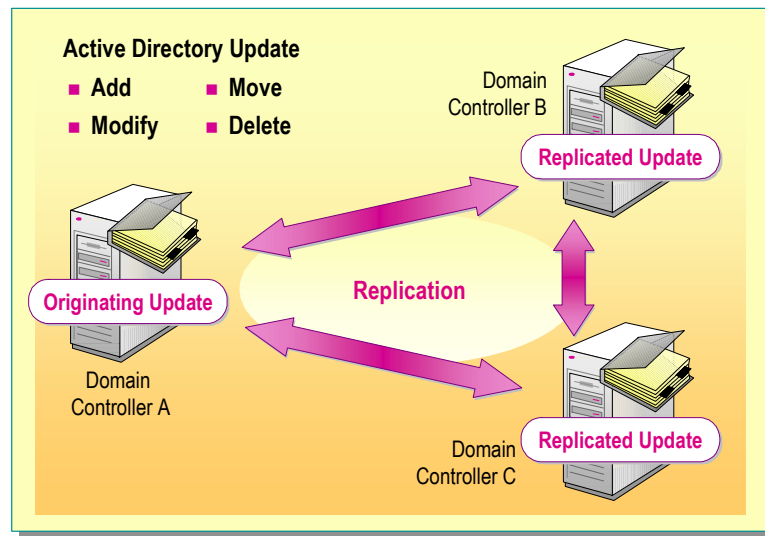
How Replication Works

Topic Objective

To identify the reasons why replication occurs, and the two types of replication updates.

Lead-in

Update requests to Active Directory are either originating updates or replicated updates.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

A committed request as a result of a change in the Active Directory database is an originating update.

An update performed at a domain controller that did not originate the update is a replicated update.

Replication of information in all domain controllers occurs because of changes made to Active Directory. Active Directory can be updated in one of the following ways:

- Adding an object to Active Directory, such as creating a new user account.
- Modifying an object's attribute values, such as changing the phone number for an existing user account.
- Modifying the name or parent of an object, and if necessary, moving the object into the new parent's domain. For example, you move the object from the sales domain to the service domain.
- Deleting an object from the directory, such as deleting user accounts for employees that no longer work for the organization.

Each update to Active Directory generates a request that can either commit or not commit to the database. A committed request is an *originating update*. After an originating update, the data must be replicated to all other replicas throughout the network.

An update performed at a domain controller that did not originate the update is called a *replicated update*. A replicated update is a committed update performed on one replica as a result of an originating or replicated update performed at another replica.

For example, when users change their passwords at Domain Controller A and Domain Controller A writes the password to the directory, this is considered an originating update. When Domain Controller A replicates the change to Domain Controller B and Domain Controller B updates its own copy of the directory, there is a replicated update at Domain Controller B.

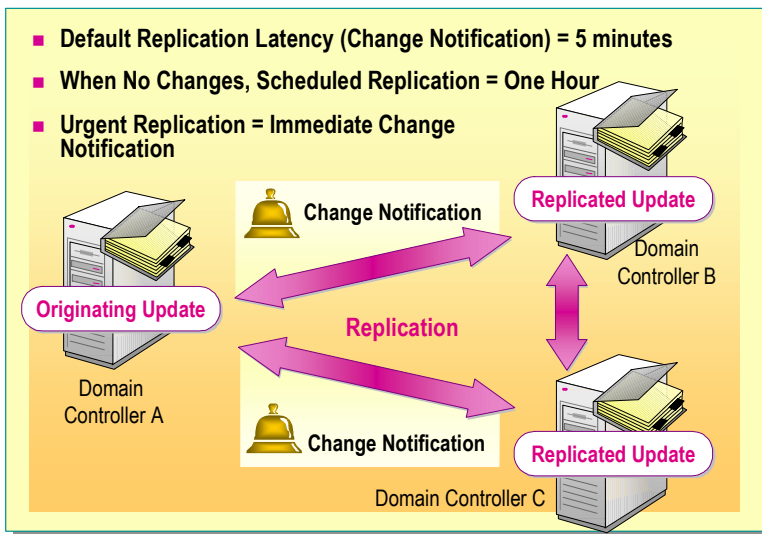
Replication Latency

Topic Objective

To illustrate the concept of replication latency during normal and urgent replication.

Lead-in

When an update is applied to a given replica, there is a replication latency before a change made on one domain controller can be received by another domain controller.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

The default replication latency period is five minutes.

The maximum propagation delay for a single change, assuming the default configuration and the three hop limit, is 15 minutes.

Urgent replication sends change notification immediately in response to urgent events instead of waiting the default period of five minutes.

Replication latency is the time needed for a change made on one domain controller to be received by another domain controller. When an update is applied to a given replica, the replication engine is triggered.

Change Notification

Replication within a site occurs through a *change notification* process. When an update occurs on a domain controller, the replication engine waits for a configurable interval, which is five minutes by default, and then sends a notification message to the first replication partner, informing it of the change. Each additional direct partner is notified after a configurable delay, which is 30 seconds by default. Thus, the maximum propagation delay for a single change, assuming the default configuration and the three hop limit (*hops* means moving data from one domain controller to another domain controller), should be 15 minutes, which may include the 30 second configurable delay. When the replication partners receive the change notification, they copy the changes from the originating domain controller.

If no changes occur during a configurable period, which is one hour by default, a domain controller initiates replication with its replication partners to ensure that no changes from the originating domain controller were missed.

Urgent Replication

Attribute changes in Active Directory that are considered security-sensitive are immediately replicated by partners being immediately notified. This immediate notification is called *urgent replication*. Urgent replication sends notification immediately in response to urgent events instead of waiting the default period of five minutes. For example, urgent replication between domain controllers is prompted is when an administrator assigns an account lockout. *Account lockout* is a security feature that sets a limit on the number of failed authentication attempts that are allowed before the account is locked out from a further attempt to log on, and a time limit for how long the lockout is in effect.

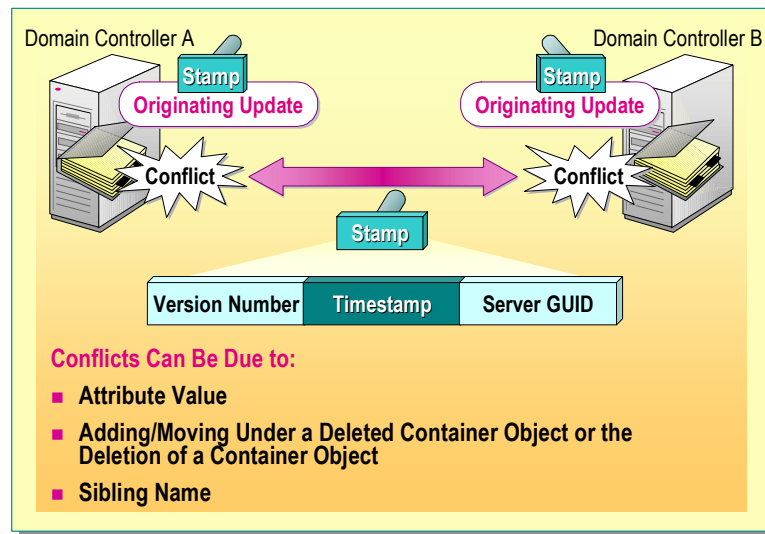
Resolving Replication Conflicts

Topic Objective

To identify why conflicts occur during replication, and how conflicts are resolved during replication.

Lead-in

Replication conflicts arise when concurrent updates originating on two separate master replicas are inconsistent.



*****ILLEGAL FOR NON-TRAINER USE*****

For timestamps to be accurate, it is important to keep the clocks on all domain controllers synchronized. But keeping time closely synchronized in a large network is difficult. Network links fail and clocks drift. Unless time is perfectly synchronized among all copies of the directory, there is a chance for data loss or directory corruption.

Active Directory replication does not depend on time to determine which changes need to be propagated. Instead, it relies on the use of USNs that are assigned by a counter that is local to each domain controller. Because these USN counters are local, it is easy to ensure that they are reliable and never decrease in value. However, you are not able to compare a USN assigned on one domain controller to a USN assigned on another domain controller. The replication system is designed with this restriction in mind.

Because replication in Active Directory is based on a multi-master model, all computers that provide multi-master updates must handle potential conflicts that may arise when concurrent updates originating on two separate master replicas are inconsistent. When the updates are replicated, these concurrent updates cause a conflict. Active Directory both minimizes and resolves conflicts.

Types of Conflicts

There are three conflict types:

- **Attribute value.** This conflict occurs when an object's attribute is set concurrently to one value at one replica, and another value at a second replica.
- **Add/move under a deleted container object or the deletion of a container object.** This conflict occurs when one replica records the deletion of a container object, while another replica records the placement of any object that is subordinate to the deleted container object.
- **Sibling name.** This conflict occurs when one replica attempts to move an object into a container in which another replica has concurrently moved another object with the same relative distinguished name.

Minimizing Conflicts

To help minimize conflicts, domain controllers record and replicate changes to objects at the attribute level rather than the object level. Therefore, changes to two different attributes of an object, such as the user's password and postal code, do not cause a conflict even if they are changed at the same time.

Globally Unique Stamps

To aid in conflict resolution, Active Directory maintains a *stamp* that contains the version number, timestamp and server globally unique identifier (GUID) created during an originating update. This stamp travels with the update as it replicates.

The stamp has the following three components in order from most to least significant:

- *Version Number*. The version number starts at one and increases by one for each originating update. When performing an originating update, the version of the updated attribute is one number higher than the version of the attribute that is being overwritten.
- *Timestamp*. The timestamp is the originating time and date of the update according to the system clock of the domain controller that performed the originating update.
- *Server GUID*. The server GUID is the originating Directory System Agent (DSA) that identifies the domain controller that performed the originating update.

Resolving Conflicts

Conflicts are resolved by assigning a globally unique stamp to all originating update operations, such as add, modify, move, or delete. If there is a conflict, the ordering of stamps allows a consistent resolution in the following ways:

- *Attribute value*. The update operation that has the higher stamp value replaces the attribute value of the update operation with the lower stamp value.
- *Add/move under a deleted container object or the deletion of a container object*. After resolution occurs at all replicas, the container object is deleted, and the leaf object is made a child of the folder's special LostAndFound container. Stamps are not involved in this resolution.
- *Sibling name*. The object with the larger stamp keeps the relative distinguished name. The sibling object is assigned a unique relative distinguished name by the domain controller. The name assignment is the relative distinguished name + "CNF:" + a reserved character (the asterisk) + the object's GUID. This name assignment ensures that the generated name does not conflict with the name of any other object.

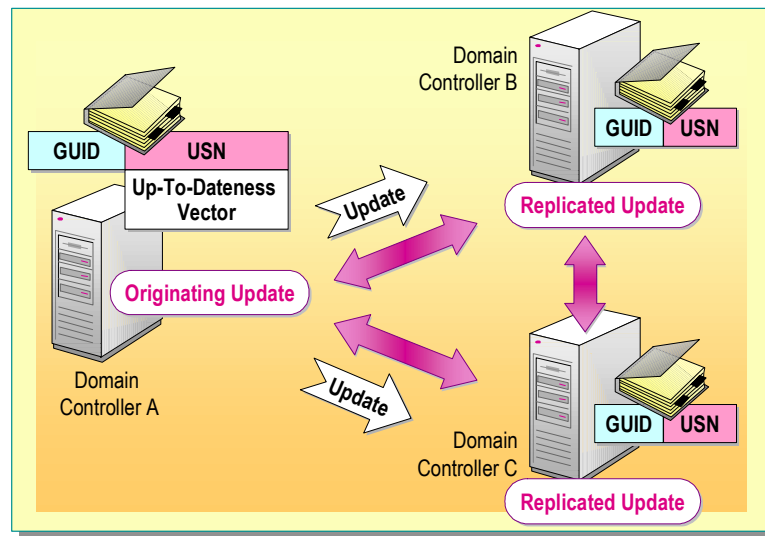
Optimizing Replication

Topic Objective

To illustrate how propagation dampening enables optimizing replication.

Lead-in

Active Directory uses propagation dampening to prevent updates from being replicated to the same domain controller more than once along different replication paths.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Points

Propagation dampening prevents updates from being replicated to the same domain controller more than once along different replication paths.

When an object is updated, there is a USN on each attribute and a USN on each object.

Up-to-dateness is the vector that is used by Active Directory to make replication efficient.

During replication, domain controllers use multiple paths for sending and receiving updates. Although using multiple paths provides both fault tolerance and improved performance, it can result in updates being replicated to the same domain controller more than once along different replication paths. To prevent these repeated replications, Active Directory replication uses *propagation dampening*. Propagation dampening is the process of reducing the amount of unnecessary data from traveling from one domain controller to another domain controller.

Update Sequence Numbers

To govern which data needs to be replicated, each domain controller maintains an array of vectors that makes replication more efficient. A *vector* is made up of a pair of data combining a GUID that is unique to each domain controller. This data is called an Invocation ID and a corresponding *update sequence number* (USN). When an object is updated, the domain controller assigns the changed USN. There is a USN on each attribute and a USN on each object. USNs are used to determine what needs to be updated in a replica. Each domain controller maintains its own distinct USN table for both originating and replicating updates.

Up-To-Dateness Vector

One of the vectors that is used by Active Directory replication is called the *up-to-dateness vector*. The up-to-dateness vector consists of database-USN pairs that are held by each domain controller, and represents the highest originating update received from each domain controller.

◆ Replication Topology

Topic Objective

To introduce the topics related to replication topology.

Lead-in

Replication topology involves the determination of which domain controller replicates with other specific domain controllers.

- Directory Partitions
- What Is Replication Topology?
- Global Catalog and Replication of Partitions
- Automatic Replication Topology Generation
- Using Connection Objects

*****ILLEGAL FOR NON-TRAINER USE*****

The actual process of replication occurs between two domain controllers at a time, and in turn, replication synchronizes information in Active Directory for the entire forest of domain controllers. Creation of replication topology involves the determination of which domain controller replicates with other specific domain controllers. When this determination is made for all domain controllers, the result is the replication topology for replication.

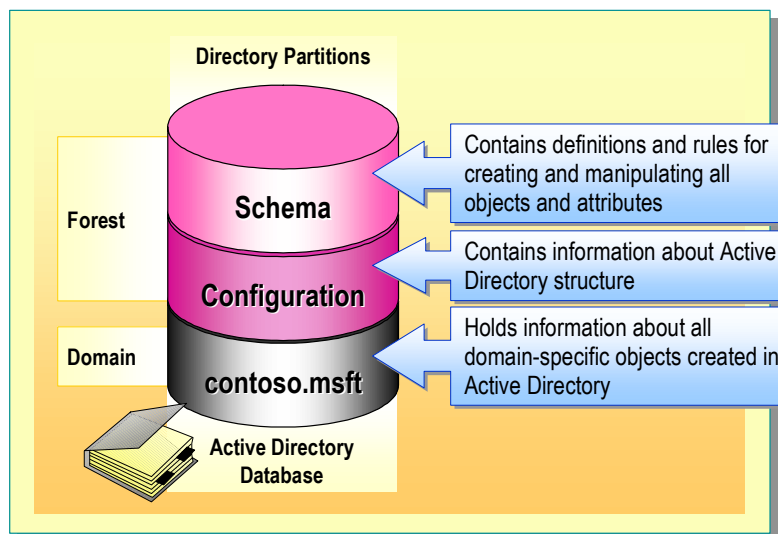
Directory Partitions

Topic Objective

To identify how the directory partitions enable replication among the domain controllers during replication.

Lead-in

The Active Directory database is logically separated into directory partitions. Each directory partition is a unit of replication.



*****ILLEGAL FOR NON-TRAINER USE*****

The slide for this topic is animated. There are three slides for this topic. In the first slide, explain the directory partitions in the Active Directory database.

The second and third slides explain the effect on replication when a domain controller is changed to a global catalog server.

Key Points

The schema partition contains definitions of all objects and attributes.

The configuration partition contains information about the Active Directory structure.

A domain partition holds information about all domain-specific objects created in Active Directory.

The Active Directory database is logically separated into directory partitions, a schema partition, a configuration partition, and domain partitions. The schema and configuration partitions are stored on all of the domain controllers of a forest. The domain partitions are stored on all of the domain controllers of the given domain. Because each partition is a unit of replication, each partition has its own replication topology. Replication is performed between directory partition replicas. Two domain controllers in the same forest often have several directory partitions in common. They always have at least two directory partitions in common, which are the schema and configuration partitions.

Schema Partition

The schema partition contains definitions of all objects and attributes that can be created in the directory, and the rules for creating and manipulating them. Schema information is replicated to all domain controllers in the forest, so regardless of the computer on which an object is created or modified, the schema partition must follow these rules. There can be only one schema per forest.

Configuration Partition

The configuration partition contains information about Active Directory structure, including what domains and sites exist, which domain controllers exist in each, and which services are available. Configuration information is replicated to all domain controllers in the forest. There can be only one configuration partition per forest.

Domain Partition

A domain partition holds information about all domain-specific objects created in Active Directory, including users, groups, computers, and organizational units. The domain partition is replicated to all domain controllers within its domain. There can be many domain partitions per forest.

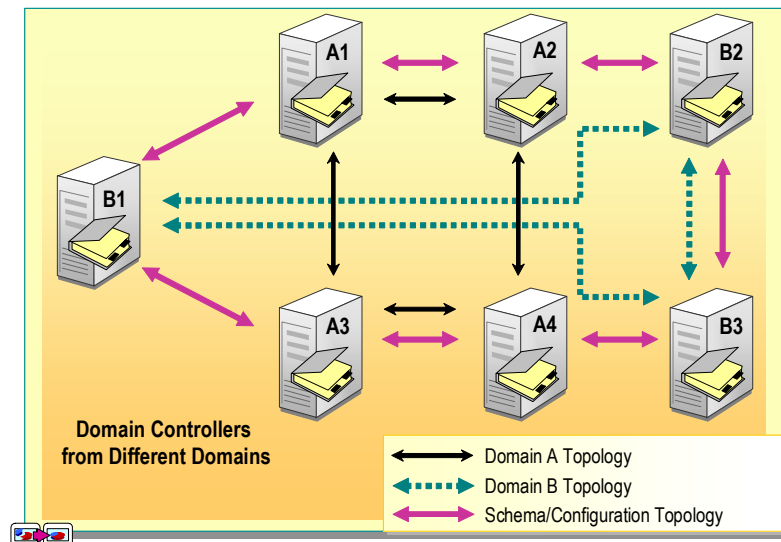
What Is Replication Topology?

Topic Objective

To illustrate the purpose of replication topology.

Lead-in

Replication topology is the pathway by which replication travels throughout a network.



*****ILLEGAL FOR NON-TRAINER USE*****

The slide for this topic is animated. There are two slides for this topic. Explain the first slide in context of all domain controllers from a single domain. The second slide explains the same concept, but the domain controllers are from two different domains. The point illustrated by the second slide is that the Schema / Configuration topology is optimized across all domain controllers regardless of the domains of which they are members.

Connection objects are present on both the source and target in replication, therefore are represented by double-sided arrows.

Key Point

A single domain controller may have different replication partners for different partitions.

Replication topology is the pathway by which replication travels throughout a network. A single domain controller may have different replication partners for different partitions. Replication topology is created on the basis of information stored in Active Directory, and can differ depending on whether you are considering schema, configuration, or domain replication. The links connecting replication partners are called *connection objects*. A connection object represents a one-way replication path between two server objects and points to the replication source.

Domain controllers that are linked by a connection object are replication partners. Replication partners can be direct or transitive. *Direct replication partners* are domain controllers that are a direct source for Active Directory replication data. A domain controller also receives replication data through *transitive replication partners*. Transitive replication partners are domain controllers whose data is obtained indirectly through a direct replication partner. You can view transitive replication partners by using the Active Directory Replication Monitor utility.

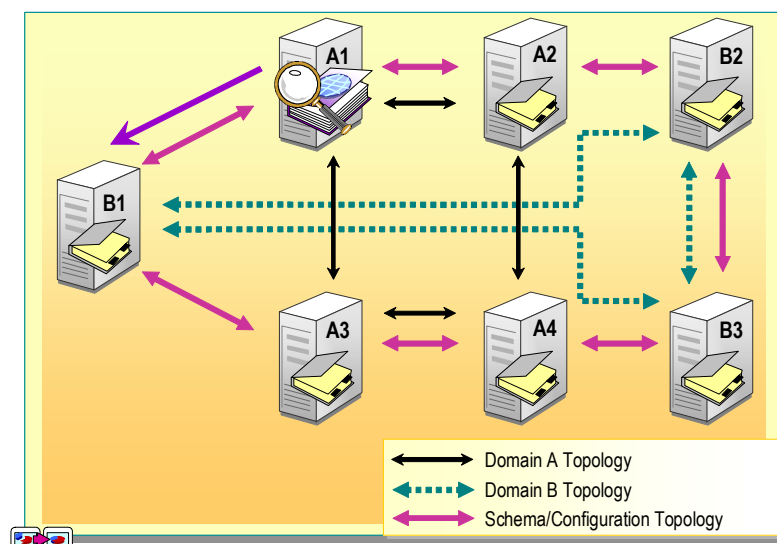
Global Catalog and Replication of Partitions

Topic Objective

To illustrate how replication topology is modified when a new global catalog sever is added to the forest.

Lead-in

Global catalog servers maintain a partial directory partition replica for all other domain partitions in the forest.



*****ILLEGAL FOR NON-TRAINER USE*****

The slide for this topic is animated. There are three slides for this topic. Use the first slide to show the directory partitions in the global catalog. Use the second and third slides to explain how replication topology changes when you add a global catalog server.

A *global catalog server* is a domain controller that stores the updatable directory partitions and a partial directory partition replica that contains a read-only copy of part of the information stored on that partition. Global catalog servers maintain a partial directory partition replica for all other domain partitions in the forest. These partial replicas contain a read-only subset, including all objects with only selected attributes, of the information in each domain partition. A full directory partition replica contains an updatable copy of all of the information stored on that partition.

When a new domain is added to the forest, the information about the new domain is stored in the configuration directory partition, which reaches the global catalog server and all domain controllers through replication of forest-wide information. Then each global catalog server becomes a partial replica of the new domain. When a new global catalog server is designated, this information is also stored in the configuration directory partition and replicated to all domain controllers in the forest, making all domain controllers aware of all of the global catalog servers in the forest.

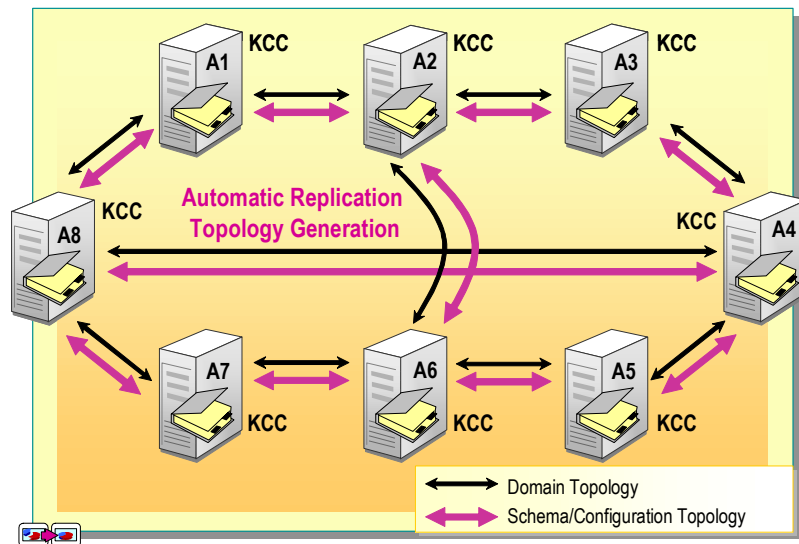
Automatic Replication Topology Generation

Topic Objective

To illustrate how KCC enables automatic replication topology generation.

Lead-in

KCC runs on each domain controller and automatically generates the replication topology for the forest.



*****ILLEGAL FOR NON-TRAINER USE*****

The slide for this topic is animated. There are two slides for this topic. Use the first slide to show the replication topology, and discuss the maximum number of hops (not more than three) it takes to replicate an originating update to all replicas of the given partition. Use the second slide to show the optimization change in topology when you add another domain controller.

When you add domain controllers to a site, there must be a method for establishing a replication path between them. Active Directory accomplishes this with replication components and a process called the *Knowledge Consistency Checker* (KCC). The KCC is a built-in process that runs on each domain controller and generates the replication topology for the forest. The KCC runs at specified intervals and designates the replication routes between domain controllers on the basis of the most favorable connections that are available at the time.

To automatically generate a replication topology, KCC uses the information on sites and subnets that belong to sites (a *subnet* is the portion of a network that shares a common address component), the cost of sending data between these sites, and the network transports that can be used between the sites. The KCC calculates the best connections between each domain controller. Additionally, if replication within a site becomes impossible or has a single point of failure, the KCC automatically establishes new connection objects as necessary to resume Active Directory replication.

The default replication topology in a site is a bidirectional ring, which is made up of two complementary unidirectional connection objects. The ring is constructed with sufficient connections so that the average maximum number of hops that are required to replicate an originating update to all replicas of the given partition does not exceed three.

Using Connection Objects

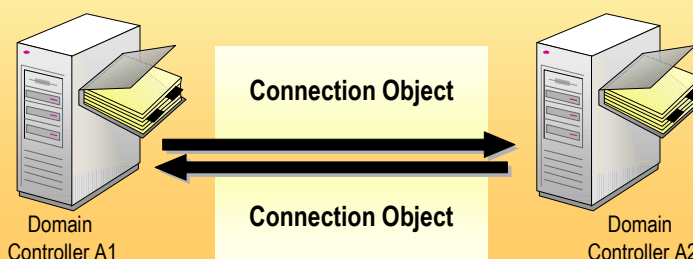
Topic Objective

To illustrate the role of connection objects in replication.

Lead-in

A connection object represents a one-way replication path between two server objects and points to the replication source.

- Connection Objects Are Created: Automatically or Manually
- Connection Objects Are Created on Each Domain Controller
- Use Active Directory Sites and Services to Manually Create, Delete, and Adjust Connection Objects
- Use the Replicate Now Option to Manually Initiate Replication



*****ILLEGAL FOR NON-TRAINER USE*****

Show students the connection objects in Active Directory Sites and Services.

Delivery Tip

Demonstrate how to manually create, delete, or adjust connection objects, or initiate replication between domain controllers.

Connection objects are created in two ways, automatically and manually. Connection objects are created automatically by running KCC on the destination domain controller. An administrator can also create connection objects manually.

Connection objects are created on each domain controller and point to another domain controller for a source of information. KCC automatically creates connection objects in pairs, making two domain controllers sources for each other. Replication from any partition uses a single connection object. For example, to fully replicate directory information between domain controller A and domain controller B, two connection objects are required. One connection object enables replication *from* domain controller A *to* domain controller B, and this connection object exists in the NTDS Settings object of domain controller B. A second connection object enables replication *from* domain controller B *to* domain controller A, and this connection object exists in the NTDS Settings object of domain controller A.

You can manually create, delete, and adjust connection objects by using Active Directory Sites and Services. You can also manually initiate replication by right-clicking a connection object in Active Directory Sites and Services and then clicking **Replicate Now**.

To manually create, delete, or adjust connection objects, or to initiate replication between domain controllers, perform the following steps:

1. Open Active Directory Sites and Services, expand **Sites**, expand **Default-First-Site-Name**, and then expand **Servers**.
2. Select the domain controller to which you want a change replicated, and then click **NTDS Settings**.
3. Right-click the connection object for the replicating partner where the change was made, click **Replicate Now**, and then click **OK**.

Lab A: Tracking Active Directory Replication

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will identify the results of the different types of replication conflicts: attribute, sibling name, and add/move under deleted container. You will also initiate replication of updates by using the connection objects for direct replication partners.



*****ILLEGAL FOR NON-TRAINER USE*****

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Identify the results of the different types of replication conflicts: attribute, sibling name, and add/move under deleted container.
- Initiate replication of updates by using the connection objects for direct replication partners.

Prerequisites

Before working on this lab, you must have the knowledge and skills to create user accounts and organizational units.

Student Computer Information

Key Points

The lab does not reflect the real-world environment. It is recommended that you always use complex passwords for any administrator accounts, and never create accounts without a password.

Outside of the classroom environment, it is strongly advised that you use the most recent software updates that are necessary. Because this is a classroom environment, we may use software that does not include the latest updates.

During this lab, you will be asked for your student number, host name, and domain. Use this information from the following table to determine what to enter for these values. Your instructor will assign you a student number.

Student number (<i>n</i>)	Host name (<i>servername</i>)	Domain (<i>domain</i>)	FQDN
1	vancouver	namerica1	vancouver.namerica1.nwtraders.msft
2	denver	namerica1	denver.namerica1.nwtraders.msft
3	perth	spacific1	perth.spacific1.nwtraders.msft
4	brisbane	spacific1	brisbane.spacific1.nwtraders.msft
5	lisbon	europa1	lisbon.europa1.nwtraders.msft
6	bonn	europa1	bonn.europa1.nwtraders.msft
7	lima	samerica1	lima.samerica1.nwtraders.msft
8	santiago	samerica1	santiago.samerica1.nwtraders.msft
9	bangalore	asia1	bangalore.asia1.nwtraders.msft
10	singapore	asia1	singapore.asia1.nwtraders.msft
11	casablanca	africa1	casablanca.africa1.nwtraders.msft
12	tunis	africa1	tunis.africa1.nwtraders.msft
13	acapulco	namerica2	acapulco.namerica2.nwtraders.msft
14	miami	namerica2	miami.namerica2.nwtraders.msft
15	auckland	spacific2	auckland.spacific2.nwtraders.msft
16	suva	spacific2	suva.spacific2.nwtraders.msft
17	stockholm	europa2	stockholm.europa2.nwtraders.msft
18	moscow	europa2	moscow.europa2.nwtraders.msft
19	caracas	samerica2	caracas.samerica2.nwtraders.msft
20	montevideo	samerica2	montevideo.samerica2.nwtraders.msft
21	manila	asia2	manila.asia2.nwtraders.msft
22	tokyo	asia2	tokyo.asia2.nwtraders.msft
23	khartoum	africa2	khartoum.africa2.nwtraders.msft
24	nairobi	africa2	nairobi.africa2.nwtraders.msft

Important The lab does not reflect the real-world environment. It is recommended that you always use complex passwords for any administrator accounts, and never create accounts without a password.

Important Outside of the classroom environment, it is strongly advised that you use the most recent software updates that are necessary. Because this is a classroom environment, we may use software that does not include the latest updates.

Estimated time to complete this lab: 15 minutes

Exercise 1

Examining Data Conflicts with Multi-Master Replication

Scenario

Northwind Traders is developing an application that uses Active Directory to store its information. The program manager is concerned that replication conflicts may have caused the application data to become corrupt.

Goal

In this exercise, you will demonstrate how replication conflicts are handled by creating the three possible conflict types, which are attribute, add/move under deleted container, and sibling name.

Note: Students will work in pairs grouped by domain to complete this exercise.

Tasks	Detailed Steps
 Important: Perform tasks 1 – 4 in this section on both <i>lowerserver</i> (where <i>lowerserver</i> is the computer with the lower student number of the pair) and <i>higherserver</i> (where <i>higherserver</i> is the computer with the higher student number of the pair) simultaneously. Read the steps for tasks 1 – 4 before proceeding. Wait until both partners are ready before proceeding. Tasks 1 – 3 need to be completed by both partners within five minutes after starting, because the normal replication time is five minutes. Any update to Active Directory starts the five-minute replication timer.	
1. Within <i>domain.nwtraders.msft</i> (where <i>domain</i> is your assigned domain name), in the Users container, create a user account with the following properties: - Full name: Duplicate_User - User logon name: Duplicate_User@nwtraders.msft	- Log on as Administrator in your domain with a password of password. - Open Active Directory Users and Computers from the Administrative Tools menu. - In the console tree, expand <i>domain.nwtraders.msft</i> (where <i>domain</i> is your assigned domain name), and then click Users. - Right-click Users, point to New, and then click User. - On the New Object – User page, in both the Full name and the User logon name boxes, type Duplicate_User and then click Next. Note: If possible, click Finish simultaneously with your partner on the next step. - Click Next, and then click Finish.
2. Create the following organizational unit (OU): <i>n_ReplOU</i> (where <i>n</i> is your assigned student number)	- Right-click <i>domain.nwtraders.msft</i>, point to New, and then click Organizational Unit. - In the New Object – Organizational Unit dialog box, in the Name box, type <i>n_ReplOU</i> (where <i>n</i> is your assigned student number) and then click OK.
3. In the <i>n_ReplOU</i> OU, create a user account with the following properties: - Full name: <i>n_ReplUser</i> - User logon name: <i>n_ReplUser@nwtraders.msft</i>	- Right-click <i>n_ReplOU</i>, point to New, and then click User. - On the New Object – User page, in both the Full name and the User logon name boxes, type <i>n_ReplUser</i> and then click Next. - Click Next, and then click Finish.

Tasks	Detailed Steps
4. Verify that the replication occurred by refreshing the display in Active Directory Users and Computers.	- Click <i>domain.nwtraders.msft</i>, and then press F5 to refresh the display. Continue to refresh the display periodically, until the <i>n_ReplOU</i> and <i>partnern_ReplOU</i> (where <i>partnern</i> is the student number of your partner's computer) organizational units are displayed, which may take five minutes to occur. - Click Users after the two organizational units are displayed.
 What happened to the two Duplicate_User user accounts? Can you tell there was a replication conflict? One account stayed the same and the other account was renamed to Duplicate_User□CNF:objectGUID (where <i>objectGUID</i> is the GUID of the object). Yes, you can tell there was a conflict by the changed name of one of the accounts.	
 Important: Perform tasks 5 – 6 on <i>lowerserver</i> only. Wait until your partner is ready to perform tasks 7 – 9 immediately after you finish task 6. Tasks 5 – 9 need to be completed within five minutes after starting. This is a result of the normal replication time of five minutes.	
5. Change the following properties of Duplicate_User:	- Right-click Duplicate_User and then click Properties. - On the General tab, in the Telephone number box, type 555-1212 - In the Office box, type 5/1093 and then click OK.
6. Delete the <i>n_ReplOU</i> OU.	Click <i>n_ReplOU</i>, press DELETE, click Yes to close the dialog box confirming the object deletion, and then click Yes again to close the dialog box confirming the deletion of all of the objects it contains.
 Important: Perform tasks 7 – 9 on <i>higherserver</i> immediately after the completion of task 6.	
7. Change the following properties of Duplicate_User:	- Right-click Duplicate_User, and then click Properties. - On the General tab, in the Telephone number box, type 123-4567 in the Description box, type Replication Test and then click OK.
8. Move <i>n_ReplUser</i> from <i>n_ReplOU</i> to <i>partnern_ReplOU</i> (where <i>partnern</i> is the student number of your partner's computer).	- Click <i>n_ReplOU</i>, right-click <i>n_ReplUser</i>, and then click Move. - In the Move dialog box, click <i>partnern_ReplOU</i>, and then click OK.

Tasks	Detailed Steps
9. Delete the <i>n_ReplOU</i> OU.	Click <i>n_ReplOU</i>, press DELETE, and then click Yes to close the dialog box confirming the object deletion.
 Important: Perform task 10 on both <i>lowerserver</i> and <i>higherserver</i> upon the completion of task 9.	
10. Verify that replication occurred by refreshing the display in Active Directory Users and Computers.	a. Click domain.nwtraders.msft, and then press F5 to refresh the display. Continue to refresh the display periodically, until both <i>n_ReplOU</i> and <i>partnern_ReplOU</i> are no longer displayed, which may take five minutes to occur. b. Click Users after the two OUs are not displayed.
 How did replication resolve the values of Telephone number, Office, and Description for Duplicate_User? The telephone number is 123-4567 because the version number was the same on both domain controllers and this value was the last written. The office number is 5/1093 and the description is Replication Test because replication is performed at the attribute level and there was no conflict.	
 What happened to the deleted organizational unit and the moved user account under it? The organizational unit was deleted. The moved user account was moved to the LostAndFound container that is located under <i>domain.nwtraders.msft</i> and can be viewed using Active Directory Users and Computers with the Advanced Features view enabled. The user account will not be in LostAndFound on <i>higherserver</i> until the next replication cycle.	

Exercise 2

Manually Initiating Replication

Scenario

The corporate testing group for Northwind Traders performs many verification tests in Active Directory. Often an update needs to replicate to another domain controller before testing continues. Manually initiating replication reduces the overall testing time.

Goal

In this exercise, you will initiate replication without having to wait for the normal replication period.

Note: Students will work in pairs grouped by domain to complete this exercise.

Tasks	Detailed Steps
 Important: Perform task 1 on <i>lowerserver</i> . Task 2 can be performed on <i>higherserver</i> simultaneously.	
1. In the LostAndFound container, delete <i>n_ReplUser</i> .	a. In Active Directory Users and Computers, click View , and then, if necessary, click Advanced Features to display advanced features. b. Click LostAndFound , in the details pane, click <i>n_ReplUser</i> , press DELETE, and then click Yes to close the dialog box confirming the object deletion.
 Important: Perform task 2 on <i>higherserver</i> . Task 1 does not need to be completed before starting task 2.	
2. Delete Duplicate_User, and Duplicate_User\CNF:objectGUID.	a. In Active Directory Users and Computers, click Users , in the details pane, click Duplicate_User , hold down the CTRL key and then click Duplicate_User\CNF:objectGUID . b. Ensuring that only the two duplicate users are selected, press DELETE, and then click Yes to close the dialog box confirming the two object deletions.
 Important: Perform task 3 on both <i>lowerserver</i> and <i>higherserver</i> upon the completion of both task 1 and task 2.	

Tasks	Detailed Steps
3. Manually initiate replication from your partner's domain controller to yours.	a. Open Active Directory Sites and Services from the Administrative Tools menu, expand Sites, expand Default-First-Site-Name, expand Servers, expand <i>servername</i> (where <i>servername</i> is the host name of your computer), and then click NTDS Settings. b. In the details pane, right-click the connection object that is from <i>partnerserver</i> (where <i>partnerserver</i> is the host name of your partner's computer), and then click Replicate Now to initiate the copying of changes from <i>partnerserver</i> to <i>servername</i>. c. Click OK to close the message indicating that replication has been initiated, and then close Active Directory Sites and Services.  <i>If an error message indicating the RPC service is unavailable occurs, simply wait a moment and then repeat the Replicate Now operation.</i>
4. Verify that replication occurred by refreshing the display in Active Directory Users and Computers and then log off.	a. In Active Directory Users and Computers, click <i>domain.nwtraders.msft</i>, and then press F5 to refresh the display. b. Click Users to verify the two duplicate users are no longer displayed, and then close Active Directory Users and Computers. c. Log off.
 Was replication performed immediately upon completion of task 3? What difference would it have made if only your partner performed task 3 and you did not? Yes, given correct operation of both domain controllers, replication occurred when it was manually initiated. It would have made a difference if only your partner had initiated replication. Your partner would have received your update, but you would not have received your partner's updates until the normal replication cycle of five minutes occurred.	

◆ Using Sites to Optimize Active Directory Replication

Topic Objective

To introduce the topics related to using sites to optimize Active Directory replication.

Lead-in

Sites enable you to control replication traffic and other types of traffic related to Active Directory across various network links.

- What Are Sites?
- Replication Within Sites
- Replication Between Sites
- Replication Protocols

*****ILLEGAL FOR NON-TRAINER USE*****

Replication ensures that all information in Active Directory is current on all domain controllers and client computers across your entire network. Many networks consist of a number of smaller networks, and the network links between these networks may operate at varying speeds. Sites in Active Directory enable you to control replication traffic and other types of traffic related to Active Directory across these various network links.

What Are Sites?

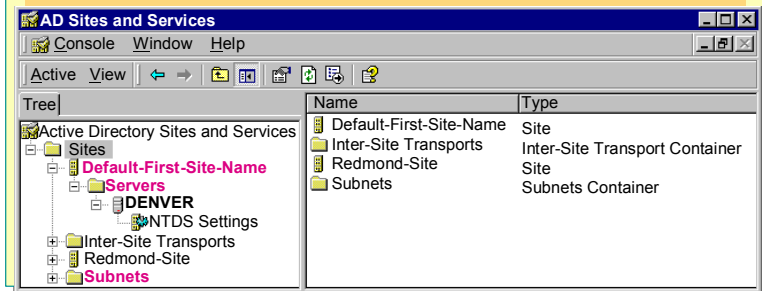
Topic Objective

To identify the purpose of sites in Active Directory.

Lead-in

Sites help to define the physical structure of a network. The first site is set up automatically when you install Windows 2000 Advanced Server on the first domain controller in a forest.

- The First Site Is Set Up Automatically, and Is Called Default-First-Site-Name
- Sites Can Consist of Zero, One, or More Subnets
- Sites Are Used to Control Replication Traffic and Logon Traffic
- Sites Contain Server Objects and Are Associated with IP Subnet Objects



*****ILLEGAL FOR NON-TRAINER USE*****

Sites can control other types of traffic, in addition to replication traffic and workstation logon traffic.

Sites help to define the physical structure of a network. A site is defined by a set of Transmission Control Protocol/Internet Protocol (TCP/IP) subnet address ranges. The first site is set up automatically when you install Windows 2000 Advanced Server on the first domain controller in a forest. The resulting first site is called *Default-First-Site-Name*. This site can be renamed.

A site can consist of no subnets or of one or more subnets. For example, in a network with three subnets in Redmond and two in Paris, the administrator can create a site in Redmond, a site in Paris, and then add the subnets to the respective sites.

A site may contain domain controllers from any domain in the forest. Sites consist of server objects. The server objects are created for a computer when it is promoted to a domain controller, and contain connection objects that enable replication.

You can use sites to control:

- *Replication traffic*. When a change occurs in Active Directory, sites can be used to control how and when the change is replicated to domain controllers in another site.
- *Logon traffic*. When a user logs on, Windows 2000 attempts to find a domain controller in the same site as the workstation.
- *Requests to Global Catalog*. When a request to a Global Catalog is required, a user computer or a Domain Controller finds a Global Catalog in the local site.

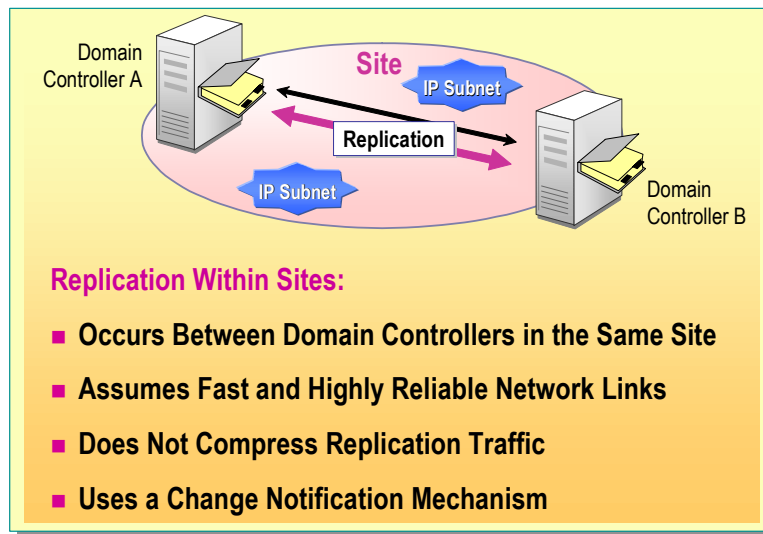
Replication Within Sites

Topic Objective

To illustrate how replication occurs within sites.

Lead-in

Replication within a site is designed to work with fast, reliable connections.



*****ILLEGAL FOR NON-TRAINER USE*****

Replication within sites occurs between domain controllers in the same site. Because a site assumes fast, highly reliable network links, replication traffic within a site is *uncompressed*. Uncompressed replication traffic helps reduce the processing load on the domain controllers. However, this uncompressed traffic can increase the network bandwidth that is required for replication messages. The network connection is assumed to be both reliable and have available bandwidth. Replication by default occurs within a site through a change notification process.

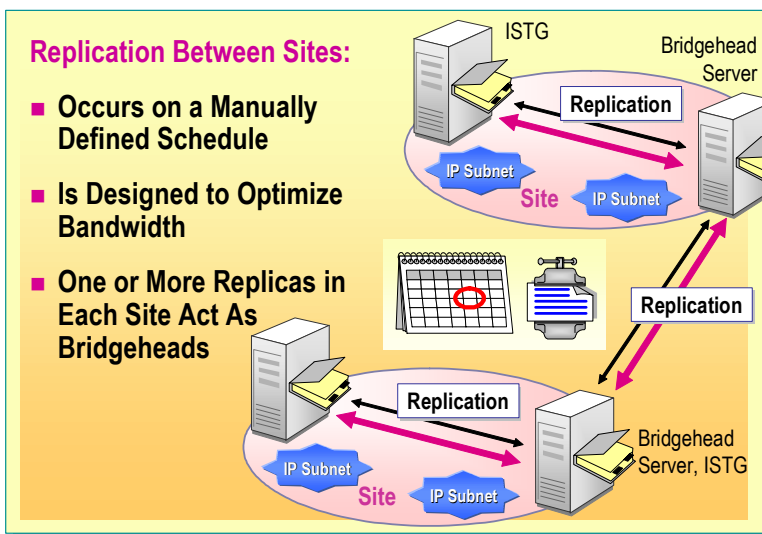
Replication Between Sites

Topic Objective

To illustrate how replication occurs between sites.

Lead-in

Replication between sites is designed under the assumption that the network links between sites have limited available bandwidth and may not be reliable.



*****ILLEGAL FOR NON-TRAINER USE*****

The ISTG domain controller cannot be manually selected.

Replication between sites is designed under the assumption that the network links between sites have limited available bandwidth and may not be reliable.

Replication Scheduling

Replication between sites happens automatically after you define configurable values, such as a schedule and a replication interval. You can schedule replication for inexpensive or off-peak hours. By default, changes are replicated between sites according to a manually defined schedule and not according to when changes occur. Configurable values, such as a schedule or an interval, define when and how often replication occurs between sites. The schedule determines at which times replication is allowed to occur, and the interval specifies how often domain controllers check for changes during the time that replication is allowed to occur.

Compressed Traffic

Replication traffic between sites is designed to optimize bandwidth by compressing all replication traffic between sites. Replication traffic is compressed to 10 to 15 percent of its original size before it is transmitted. Although compression optimizes network bandwidth, it imposes an additional processing load on domain controllers.

Bridgehead Servers

When replication occurs between sites, one or more replicas in each site act as bridgeheads to another site in the topology. A server is automatically designated as a bridgehead server by using the Intersite Topology Generator (ISTG) in each site to perform replication between sites. After replication between sites is completed by using the bridgehead server, the bridgehead servers communicate all updates to all domain controllers within their sites by using the normal replication process.

If you want to restrict the domain controllers in which the ISTG can create connections between sites, select one or more domain controllers in the site that you want the ISTG to always consider as *preferred bridgehead servers*. These servers are used to replicate the changes from the site.

If the bridgehead server becomes unavailable, another bridgehead server is automatically chosen from the list of preferred bridgehead servers.

To verify which domain controller has the role of ISTG, perform the following steps:

1. In Active Directory Sites and Services, select a site in the Sites folder.
2. In the details pane, right-click the **NTDS Site Settings** object, and then click **Properties**.

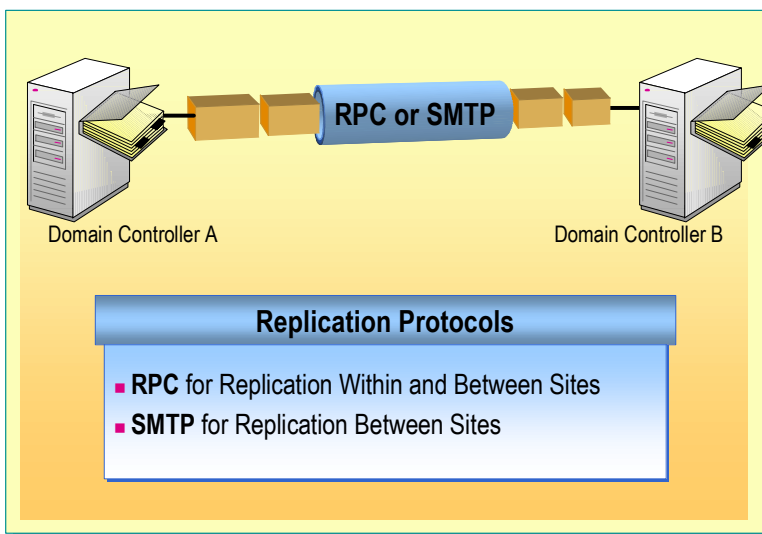
Replication Protocols

Topic Objective

To illustrate how replication transports provide the protocols required for data transfer.

Lead-in

Active Directory requires a network protocol for replication traffic.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate the replication protocols by using Active Directory Sites and Services.

Key Point

If replication uses the SMTP protocol, the information can be stored and forwarded to many mail servers until it reaches the destination domain controller at a later time. Therefore, a connection does not need to be established directly between the two replicating domain controllers.

To ensure that computers in a network are able to communicate for sending and receiving updates during replication, they must share a common language known as a *replication protocol*. Within a single site, there is only one protocol used for replication. In a multiple-site structure, you must select one of the following replication protocols for replication between sites.

- *Remote procedure call (RPC)*. Active Directory replication uses RPC over IP for replication within a site. RPC is an industry standard protocol for client/server communications that is compatible with most types of networks. For replication within a site, RPC provides uniform, high-speed connectivity. When you configure replication between sites, you must choose between replication protocols, RPC over IP, or the Simple Mail Transfer Protocol (SMTP). However, the domain controllers must be in different domains and in different sites for you to use SMTP. In most cases, choose RPC over IP for replication between sites.
- *Simple mail transfer protocol (SMTP)*. SMTP supports schema configuration and global catalog replication but cannot be used to replicate the domain partition to domain controllers of the same domain. This is because some domain operations, for example Group Policy, require the support of the File Replication service (FRS), which does not yet support an asynchronous transport for replication. You need to use RPC for replicating the domain partition. A feature of SMTP replication is that a connection does not need to be established directly between the two replicating domain controllers. Instead, the information can be stored and forwarded to many mail servers until it reaches the destination domain controller at a later time.

Note Active Directory Sites and Services labels the protocol for connections within a site as RPC and the protocol for connections between sites as IP. Both labels, however, mean that the connection uses RPC over IP.

◆ Implementing Sites to Manage Active Directory Replication

Topic Objective

To introduce the topics related to implementing sites to manage Active Directory replication.

Lead-in

In a small network, implementing sites may be as simple as renaming the default site that the Active Directory Installation wizard creates. But in a larger network, implementing an efficient physical structure can involve creating sites, subnets, site links, and site link bridges.

- **Creating Sites and Subnets**
- **Creating and Configuring Site Links**
- **Creating a Site Link Bridge**

*****ILLEGAL FOR NON-TRAINER USE*****

You can use subnets, site links, and site link bridges to help control the replication topology when configuring replication between sites. An efficient, reliable replication topology depends on the configuration of site links and site link bridges. You use Active Directory Sites and Services to create sites, subnets, site links, and site link bridges.

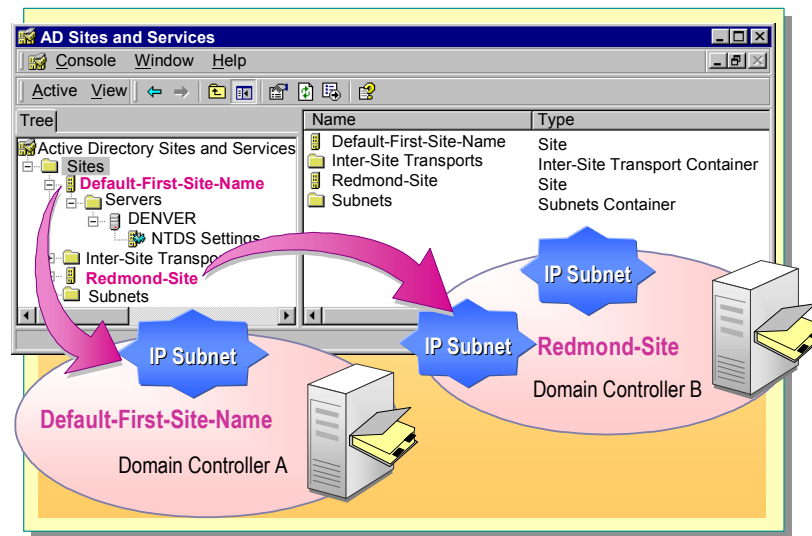
Creating Sites and Subnets

Topic Objective

To illustrate how to create sites and subnets.

Lead-in

Site creation is a simple process. After you define a site, you create a subnet object.



*****ILLEGAL FOR NON-TRAINER USE*****

The naming rules for sites are: you can use 63 English characters, and the site name can contain letters (a-z, A-Z), numbers (0-9) and hyphens (-). It cannot contain spaces, periods (.) or only numbers. If an underscore is used, an error message will ask if you want to still use the underscore and not be in compliance with DNS standards.

Delivery Tips

Demonstrate how to create a site.

Demonstrate how to create a subnet object and associate it with the newly created site.

Key Point

To create sites, you must log on as a member of the Enterprise Admins group, or use the Secondary Logon service to start Active Directory Sites and Services.

Computers on TCP/IP networks are assigned to sites based on the TCP/IP to which they have been configured. Because subnets group well-connected computers together, subnets are useful for identifying sites. To use sites for managing replication within or between sites, you create additional sites and subnets.

Creating a Site

To create a site, you must provide a name for the new site and associate the site with a site link. You must log on as a member of the Enterprise Admins group to create sites, or use the Secondary Logon service to start Active Directory Sites and Services in the security context of a member of the Enterprise Admins group.

To create a site, perform the following steps:

1. Open Active Directory Sites and Services from the **Administrative Tools** menu, in the console tree, right-click **Sites**, and then click **New Site**.
2. In the **Name** box, type the name of the new site.
3. Click a site link object, and then click **OK**.

Note Select the default site link if it is the only link available.

Creating a Subnet Object

After you define your sites, you create subnets and associate them with sites. The operating system and applications use subnet information to reduce network traffic by finding the closest server to the client. Subnet information is used during the process of domain controller location to find a domain controller in the same site as the computer that is logging on.

To create a subnet object, perform the following steps:

1. Open Active Directory Sites and Services from the **Administrative Tools** menu, and then in the console tree, double-click **Sites**.
2. Right-click **Subnets**, and then click **New Subnet**.
3. In the **Address** box, enter the subnet address.
4. In the **Mask** box, enter the subnet mask that describes the range of addresses included in this site's subnet.
5. Choose a site with which to associate this subnet, and then click **OK**.

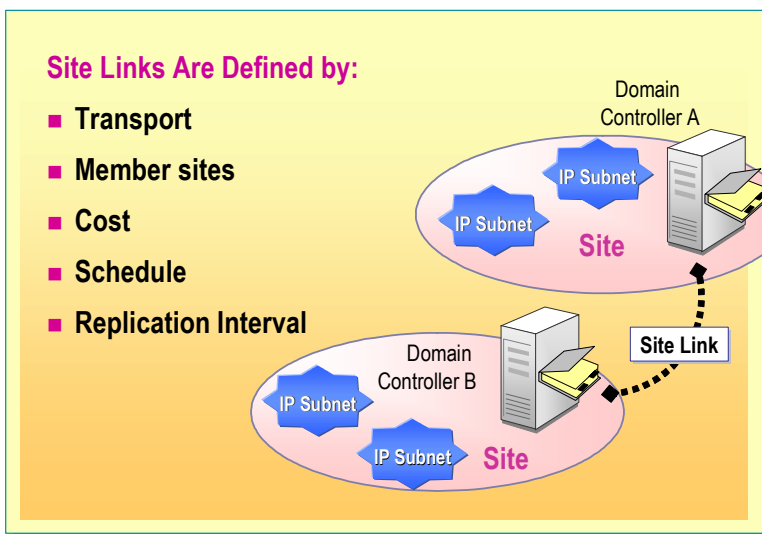
Creating and Configuring Site Links

Topic Objective

To illustrate how to create and configure site links.

Lead-in

A site link represents a connection between sites to be used for replication.



*****ILLEGAL FOR NON-TRAINER USE*****

Point out to the students the site links that are created in Active Directory Sites and Services.

Replication recognizes schedule intervals of 15 minutes; however, you cannot set this interval in the user interface.

Delivery Tip

Demonstrate how to create a site link.

Demonstrate how to configure a site link.

A *site link* is an object used to manage replication between sites. You can create site links that allow domain controllers from one site to replicate with the other site. Site links are defined by the following components:

- *Transport*. The networking technology that is used to transfer the data that is replicated.
- *Member sites*. Two or more sites that will be connected through the site link.
- *Cost*. Site link cost is a number that represents the priority an organization assigns to replication traffic between the sites. Cost reflects the speed and reliability of the underlying network. If there are multiple site links between two sites, replication will use the link with the lowest cost that is available. The cost ranges between one and 32767.
- *Schedule*. The times when replication will occur. Schedule defines a time range when replication is allowed over the link. The schedule range is one hour for a seven-day week.
- *Replication interval*. Replication interval defines how often replication occurs in a given schedule window. Replication intervals can range from 15 to 10,080 minutes.

Creating Site Links

After you configure the sites for your network, you create site links in Active Directory to map the connections between the sites. You can define the schedule according to the most beneficial time for replication to occur on the basis of network traffic and cost. Create site links that use a specific inter-site transport. These site links are either RPC or SMTP.

To create a site link, perform the following steps:

1. Open Active Directory Sites and Services from the **Administrative Tools** menu, and then double-click **Inter-Site Transport**.
2. Right-click the inter-site transport protocol that you want the site link to use, and then click **New Site Link**.
3. In the **Name** box, type the name to be given to the link.
4. Click two or more sites to connect, and then click **Add**.
5. Configure the site link's cost, schedule, and replication interval.

Configuring Site Links

Cost, replication interval, and schedule are properties of the site link. When you create the site link, these properties are set to the default values. The default value of cost is 100 and of replication interval is three hours, and the schedule available for replication is all periods of time.

To configure site links, perform the following steps:

1. Open Active Directory Sites and Services from the **Administrative Tools** menu, expand **Sites**, and then double-click **Inter-Site Transports**.
2. Click **IP** or **SMTP**, depending on which protocol the site link is configured to use.
3. Right-click the site link, and then click **Properties**.
4. On the **General** tab of the **Properties** dialog box, change the values for cost, replication interval, and schedule as needed, and then click **OK**.

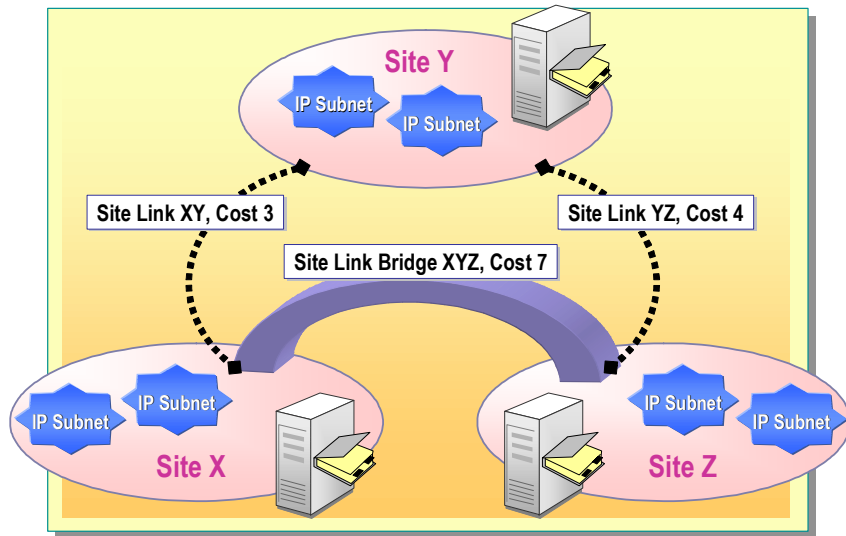
Creating a Site Link Bridge

Topic Objective

To illustrate how to create a site link bridge.

Lead-in

In a fully routed network, you do not need to create site link bridges manually.



*****ILLEGAL FOR NON-TRAINER USE*****

Multiple site link bridges work independently of one another.

Delivery Tip

Demonstrate how all site links are bridged by default.

Demonstrate how to create a site link bridge.

A *site link bridge* consists of two or more site links. Site link bridges are used to connect two or more sites together and model the routing behavior of a network. The site link bridge enables transitivity between site links. By default, all site links are transitive; you do not need to create any site link bridges. You can turn off the Bridge all site links feature and manually create site link bridges that you require.

How to Create a Site Link Bridge

A site link bridge object for a specific transport between sites is created by specifying two or more site links. For example:

- Site link XY connects sites X and Y through an IP with a cost of 3.
- Site link YZ connects sites Y and Z through an IP with a cost of 4.
- Site link bridge XYZ connects XY and YZ.

The site link bridge XYZ implies that an IP message can be sent from site X to site Z directly with a cost of 3 plus 4, or 7. TCP/IP routing dictates the actual path that the message travels. Each site link in a bridge needs to have a site in common with another site link in the bridge. If not, the bridge cannot compute the cost from sites in the link to the sites in other links of the bridge.

To create a site link bridge, perform the following steps:

1. Open Active Directory Sites and Services from the **Administrative Tools** menu, expand **Sites**, and then in the console tree, right-click the inter-site transport folder for which you want to create a new site link bridge.
2. Right-click either **IP** or **SMTP**, depending on the protocol for which you want to create a site link bridge, and then click **New Site Link Bridge**.
3. In the **Name** box, type a name for the site link bridge.
4. Click two or more site links to be bridged, click **Add**, and then click **OK**.

When to Create a Site Link Bridge

You usually turn off the Bridge all site links feature and manually define site link bridges in the following two situations:

- There may be sites that are not in a fully-routed IP network. This means that domain controllers in one site cannot directly communicate with domain controllers in another site because of an IP routing constraint. This situation occurs when you use internal firewalls. For example, in the illustration on the slide, if a domain controller in site X cannot communicate directly with a domain controller in site Z, you turn off the Bridge all site links feature. If you have more site links that should be bridged, add more site link bridges to all site links excluding the site links XY and YZ, which contain the IP networks that cannot communicate directly with each other.
- There may be too many sites for the KCC on the ISTG domain controllers to calculate the topology on a schedule. If there are many topology connection paths, which are actually not required because better connection paths exist, reduce the number of possible connection paths to improve performance. To do this, turn off the Bridge all site links feature. Then add more site link bridges if required. Alternatively, you can turn off the KCC for topology generation between sites. However, turning off the KCC will not recalculate the topology if a site becomes unavailable and you will need to manually reconfigure the topology.

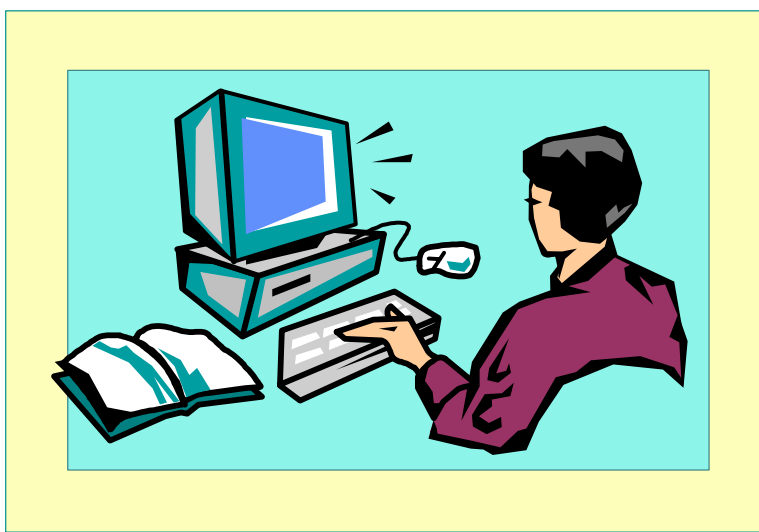
Lab B: Using Sites to Manage Active Directory Replication

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will create a site, subnet, site link, and site link bridge, and then configure site link properties.



*****ILLEGAL FOR NON-TRAINER USE*****

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Create a site, subnet, site link, and site link bridge.
- Configure the properties of a site link.

Prerequisites

Before working on this lab, you must have an understanding of TCP/IP subnets.

Student Computer Information

During this lab, you will be asked for your student number, host name, and IP address. Use this information from the following table to determine what to enter for these values. Your instructor will assign you a student number and the classroom network ID *x*.

Student number (<i>n</i>)	Host name (<i>servername</i>)	Domain (<i>domain</i>)	FQDN
1	vancouver	namerica1	vancouver.namerica1.nwtraders.msft
2	denver	namerica1	denver.namerica1.nwtraders.msft
3	perth	spacific1	perth.spacific1.nwtraders.msft
4	brisbane	spacific1	brisbane.spacific1.nwtraders.msft
5	lisbon	europa1	lisbon.europa1.nwtraders.msft
6	bonn	europa1	bonn.europa1.nwtraders.msft
7	lima	samerica1	lima.samerica1.nwtraders.msft
8	santiago	samerica1	santiago.samerica1.nwtraders.msft
9	bangalore	asia1	bangalore.asia1.nwtraders.msft
10	singapore	asia1	singapore.asia1.nwtraders.msft
11	casablanca	africa1	casablanca.africa1.nwtraders.msft
12	tunis	africa1	tunis.africa1.nwtraders.msft
13	acapulco	namerica2	acapulco.namerica2.nwtraders.msft
14	miami	namerica2	miami.namerica2.nwtraders.msft
15	auckland	spacific2	auckland.spacific2.nwtraders.msft
16	suva	spacific2	suva.spacific2.nwtraders.msft
17	stockholm	europa2	stockholm.europa2.nwtraders.msft
18	moscow	europa2	moscow.europa2.nwtraders.msft
19	caracas	samerica2	caracas.samerica2.nwtraders.msft
20	montevideo	samerica2	montevideo.samerica2.nwtraders.msft
21	manila	asia2	manila.asia2.nwtraders.msft
22	tokyo	asia2	tokyo.asia2.nwtraders.msft
23	khartoum	africa2	khartoum.africa2.nwtraders.msft
24	nairobi	africa2	nairobi.africa2.nwtraders.msft

Estimated time to complete this lab: 30 minutes

Exercise 1

Creating IP Subnet and Site Objects

Scenario

Northwind Traders is geographically distributed with many wide area network (WAN) links that connect these regions. Network bandwidth on these WAN links is scarce. Active Directory must be aware of which connections are local area network (LAN) and which are WAN to optimize replication and minimize the use of the network across WAN links. You will create IP subnet and site objects and associate subnets to sites.

Goal

In this exercise, you will create IP subnet and site objects in Active Directory. You will associate subnets with sites. This association informs Active Directory which IP subnets have high network bandwidth such as a LAN.

Note: Because of the limitations of the classroom setup, you will be creating subnet objects that do not match the classroom network. Therefore, the normal configuration step of moving the server objects into the new sites will not be performed in this lab.

Tasks	Detailed Steps
1. Create a new site with the name <i>servernameSite</i> (where <i>servername</i> is the host name of your computer) and link it to DEFAULTSITE LINK.	- Log on as Administrator in your domain with a password of password. - Click Start, point to Programs, point to Administrative Tools, hold down the SHIFT key and right-click Active Directory Sites and Services, and then click Run as. - In the Run As Other User dialog box, type Administrator in the User name box, type password in the Password box, type nwtraders.msft in the Domain box, and then click OK. - In the AD Sites and Services window, in the console tree, verify that Active Directory Sites and Services [london.nwtraders.msft] appears. - In the console tree, right-click Sites, and then click New Site. - In the New Object – Site dialog box, in the Name box, type <i>servernameSite</i> (where <i>servername</i> is the host name of your computer). - Under Link Name, click DEFAULTSITE LINK, click OK, and then click OK again to close the message indicating that further configuration may need to be performed.
2. Create a new subnet object with the network ID of 10.10.<i>n</i>.0 (where <i>n</i> is your assigned student number), and a subnet mask of 255.255.255.0 . Associate this subnet object with your site <i>servernameSite</i> .	- In Active Directory Sites and Services, expand Sites, right-click Subnets, and then click New Subnet. - In the New Object – Subnet dialog box, in the Address box, type 10.10.<i>n</i>.0 (where <i>n</i> is your assigned student number). - In the Mask box, type 255.255.255.0. - Under Site Name, click <i>servernameSite</i>, and then click OK. - Leave Active Directory Sites and Services open.

Exercise 2

Creating Site Links and Site Link Bridges

Scenario

The physical network of Northwind Traders has been used to create the Active Directory IP subnet and site objects. The sites on the corporate network backbone have already been configured. The site links and site link bridges need to be established to connect the remote sites to the corporate backbone sites. The Bridge all site links feature will be turned off by the corporate administrators after the site links and site link bridges for all remote sites have been configured and verified. You must create and configure the site link and site link bridge from your remote site to connect to the corporate backbone.

Goal

In this exercise, you will create IP site links between your site and Default-First-Site-Name. You will configure the replication time window and frequency and the cost of the links. You will create a site link bridge that connects your site link to DEFAULTIPSITELINK.

The DEFAULTIPSITELINK will represent the site link used to connect all of the corporate backbone sites. The Default-First-Site-Name will represent the main corporate site. The reason for creating site link bridges is to reduce processing requirements on the inter-site topology generator servers. Another reason is that a more deterministic replication path will result because all of the remote sites will only use the corporate backbone as the central hub for replication.

Tasks	Detailed Steps
1. Create a new IP site link called <i>servernameSite-CorpHQ</i> and add the sites Default-First-Site-Name and <i>servernameSite</i> .	- In Active Directory Sites and Services, expand Sites, expand Inter-Site Transports, and then click IP. - Right-click IP, and then click New Site Link. - In the New Object – Site Link dialog box, in the Name box, type <i>servernameSite-CorpHQ</i>. - In the Sites not in this site link box, click Default-First-Site-Name, click Add, click <i>servernameSite</i>, click Add, and then click OK.
2. Configure the <i>servernameSite-CorpHQ</i> site link with a cost of 500, a frequency of 90 minutes, and a daily schedule of 11 P.M. to 6 A.M.	- Click IP, and in the details pane, right-click <i>servernameSite-CorpHQ</i>, and then click Properties. - In the <i>servernameSite-CorpHQ Properties</i> dialog box, in the Cost box, type 500. - In the Replicate every minutes box, type 90. - Click Change Schedule. - In the Schedule for <i>servernameSite-CorpHQ</i> dialog box, select Sunday through Saturday, 6 AM to 10 PM, click Replication not Available, click OK, and then click OK again to close the <i>servernameSite-CorpHQ Properties</i> dialog box.

Tasks	Detailed Steps
3. Create a new site link bridge called <i>servernameSite-CorpHQ-Bridge</i> between <i>servernameSite-CorpHQ</i> and DEFAULTIPSITELINK .	a. Right-click IP, and then click New Site Link Bridge. b. In the New Object – Site Link Bridge dialog box, in the Name box, type <i>servernameSite-CorpHQ-Bridge</i> c. Ensure that <i>servernameSite-CorpHQ</i>, and DEFAULTIPSITELINK are listed in the Site links in this site link bridge box. If there are no site links listed, in the Site links not in this site link bridge box, click <i>servernameSite-CorpHQ</i>, click Add, click DEFAULTIPSITELINK, click Add, and then click OK.
4. Remove <i>servernameSite</i> from DEFAULTIPSITELINK , and then log off.	a. Click IP, and in the details pane, right-click DEFAULTIPSITELINK, and then click Properties. b. In the DEFAULTIPSITELINK Properties dialog box, in the Sites in this Site link box, click <i>servernameSite</i>, click Remove, and then click OK. c. Close Active Directory Sites and Services, close all open windows, and then log off.

◆ Monitoring Replication Traffic

Topic Objective

To introduce the topics related to monitoring replication traffic.

Lead-in

Monitoring replication traffic can help you determine the most efficient topology for your network.

- What Is Replication Monitor?
- Using Replication Monitor to Monitor Replication Traffic
- Using Repadmin to Monitor Replication Traffic

*****ILLEGAL FOR NON-TRAINER USE*****

You can adjust your replication topology based on replication traffic patterns. To help adjust replication traffic patterns, you need to be able to view the replication traffic throughout your network. You can view replication traffic by using Replication Monitor and the **repadmin** command-line utility.

What Is Replication Monitor?

Topic Objective

To identify the reasons to monitor replication traffic by using Replication Monitor.

Lead-in

Replication Monitor provides a display of your replication topology.

With Replication Monitor You Can:

- Display the Replicating Partner
- Display Each USN Value, the Number of Failed Attempts, Reason, and Flags
- Poll the Server at an Administrator-Defined Interval
- Monitor the Count of Failed Replication Attempts
- Show Which Objects Have Not Yet Replicated
- Synchronize Between Just Two Domain Controllers
- Trigger the KCC into Recalculating the Replication Topology

*****ILLEGAL FOR NON-TRAINER USE*****

Replication Monitor displays in graphical format the replication topology of connections between servers on the same site. It enables administrators to view low-level status and performance of replication between Active Directory domain controllers. It also includes functions that are wrapped application programming interfaces (APIs) to make it easy to write a replication script with just a few lines of code.

With Replication Monitor, you can:

- See which computers are replicating information both directly and transitively.
- Display each USN value, the number of failed replication attempts, the reason for failed attempts, and the flags used for direct replication partners. If the failure meets or exceeds an administrator-defined value, it can write to an event log and send mail.
- Poll the server at an administrator-defined interval to get current statistics and replication state, and to save a log file history.
- Allow administrators to show which objects have not yet replicated from a particular computer.
- Allow administrators to synchronize between two domain controllers.
- Allow administrators to use the KCC to recalculate the replication topology.

You can run the Replication Monitor utility on any domain controller, member server, or stand-alone computer that runs Windows 2000 Advanced Server.

Note For more information about Replication monitoring in Active Directory, see the Windows 2000 Help.

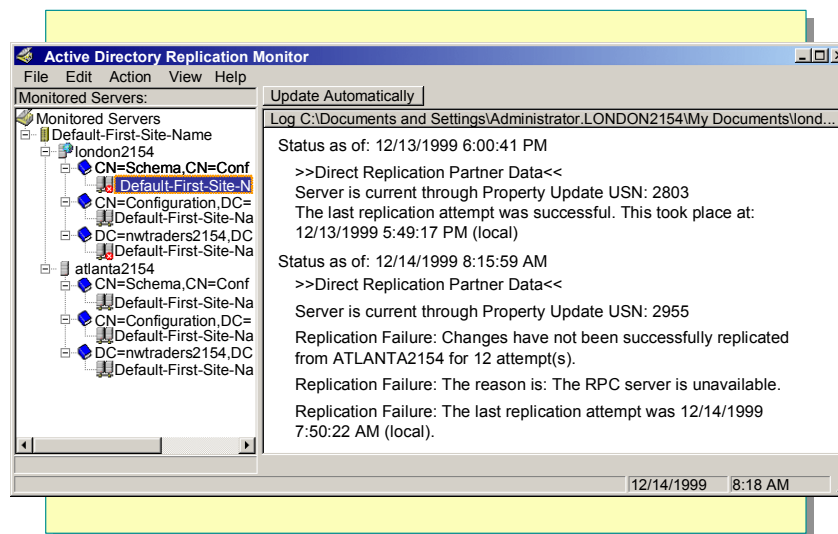
Using Replication Monitor to Monitor Replication Traffic

Topic Objective

To illustrate how to monitor replication traffic by using Replication Monitor.

Lead-in

You use Replication Monitor to view replication between domain controllers in a domain.



*****ILLEGAL FOR NON-TRAINER USE*****

Explain to the students the output of Replication Monitor as shown in the slide.

Delivery Tip

Demonstrate how to start and configure Replication Monitor.

Use Replication Monitor to view replication between domain controllers in a domain. To start and configure Replication Monitor, perform the following steps:

1. On the **Start** menu, point to **Programs**, point to **Windows 2000 Support Tools**, click **Tools**, and then click **Active Directory Replication Monitor**.
2. On the **View** menu, click **Options**.
3. On the **Active Directory Replication Monitor Options** page, click the **Status Logging** tab, click **Display Changed Attributes when Replication Occurs**, and then click **OK**.
4. Right-click **Monitored servers**, and then click **Add Monitored Server**.
5. In the Add Server to Monitor wizard, click **Add the server explicitly by name**, and then click **Next**.
6. In the **Enter the name of the server to monitor explicitly** box, type the server name, and then click **Finish**.

Using Repadmin to Monitor Replication Traffic

Topic Objective

To illustrate how to monitor replication traffic by using **repadmin**.

Lead-in

You can also use the **repadmin** command to view the replication topology from the perspective of each domain controller.

```
C:\WINNT\System32\cmd.exe
C:\>repadmin /showreps denver.domain2.nwtraders.msft

Default-First-Site-Name\DENVER
DSA Options : IS_GC
objectGuid : c2f675f8-9f03-4ad0-8ec7-55d9da972162
invocationID: 4072f8c8-2446-4421-831b-d493a81d1418

===== INBOUND NEIGHBORS =====
CN=Schema,CN=Configuration,DC=domain2,DC=nwtraders,DC=msft
  Default-First-Site-Name\SERVER2 via RPC
  objectGuid: 179fff42-4345-4c5f-a09f-ad641b564199
  Last attempt @ 2000-01-03 09:59:19 was successful.
CN=Configuration,DC=domain2,DC=nwtraders,DC=msft
  Default-First-Site-Name\SERVER2 via RPC
  objectGuid: 179fff42-4345-4c5f-a09f-ad641b564199
  Last attempt @ 2000-01-03 10:02:25 was successful.
DC=domain2,DC=nwtraders,DC=msft
  Default-First-Site-Name\SERVER2 via RPC
  objectGuid: 179fff42-4345-4c5f-a09f-ad641b564199
  Last attempt @ 2000-01-03 09:59:18 was successful.

===== OUTBOUND NEIGHBORS FOR CHANGE NOTIFICATIONS =====
CN=Schema,CN=Configuration,DC=domain2,DC=nwtraders,DC=msft
  Default-First-Site-Name\SERVER2 via RPC
  objectGuid: 179fff42-4345-4c5f-a09f-ad641b564199
CN=Configuration,DC=domain2,DC=nwtraders,DC=msft
  Default-First-Site-Name\SERVER2 via RPC
  objectGuid: 179fff42-4345-4c5f-a09f-ad641b564199
DC=domain2,DC=nwtraders,DC=msft
  Default-First-Site-Name\SERVER2 via RPC
  objectGuid: 179fff42-4345-4c5f-a09f-ad641b564199
C:\>
```

*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

Demonstrate how to run **repadmin** at the command prompt.

Administrators use the **repadmin** command to view the replication topology from the perspective of each domain controller. You can also use the **repadmin** command to manually create the replication topology, force replication events between domain controllers, and view both the replication metadata, which is information about the data, and up-to-dateness vectors.

To run the **repadmin** command, perform the following step:

- At the command prompt, type
repadmin command arguments [/u:{domain\}user /pw:{password}*}]

The following examples use some of available command arguments for the **repadmin** command:

- To display the replication partners for domain controller named domaincontroller1, use the syntax
repadmin /showreps domaincontroller1.contoso.msft
- To display the highest Update Sequence Number on the domain controller named domaincontroller2, use the syntax
repadmin /showvector dc=contoso,dc=msft domaincontroller2.contoso.msft
- To display the connection objects for the domain controller named domaincontroller1, use the syntax
repadmin /showconn server2.microsoft.com

Note For more information about the arguments that can be used with the **repadmin** command, you can read the usage statement, which is obtained by running **repadmin /?** at the command prompt.

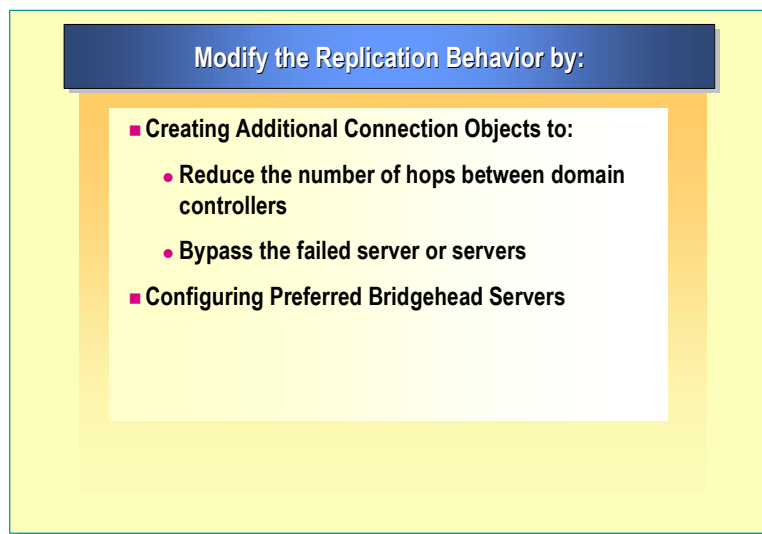
Adjusting Replication

Topic Objective

To illustrate the adjustments that can be made to improve replication performance.

Lead-in

The replication process is automatic, therefore the default replication topology requires only infrequent adjustments.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tips

Demonstrate how to create additional connection objects.

Demonstrate how to limit which servers ISTG can designate as bridgeheads.

Active Directory replication occurs automatically and reliably with no administrative intervention, other than that required to configure sites and site links. An administrator can use Active Directory Sites and Services to modify a replication topology by adding or removing connection objects, and limit ISTG's choices of bridgeheads.

Creating Additional Connection Objects

Generally, you manually create connection objects only if the connections that KCC creates do not connect domain controllers that an administrator wants connected. The following situations may require additional connections between domain controllers within a site or between sites:

- When you want to reduce the number of hops from the default of three to one or two hops between domain controllers within a site.
- When failures occur between domain controllers in different sites. If failures occur, KCC detects the failures and automatically reroutes connections to bypass the failed server or servers.

Note Before you create additional connections, it is important to consider the cost of the additional connections compared with the cost of the default configuration.

When you modify the connection objects, the following rules apply:

- The KCC will not automatically delete a connection object that has been manually created.
- If you create a connection to the same server that the KCC would normally create, the KCC will not create an additional connection.
- At any time, if a domain controller can not get updates from its current replication partners, it will use the KCC to establish as many new connection objects as necessary to other domain controllers to resume Active Directory replication.

Configuring Preferred Bridgehead Servers

You can limit the choice of servers that ISTG can designate as bridgeheads by selecting one or more domain controllers in the site that you contains the servers that you want ISTG to always consider as preferred bridgehead servers.

Emphasize that it is recommended always to have more than one preferred bridgehead server so that the ISTG can select an alternate server if one fails.

To limit ISTG's choices of bridgeheads, perform the following steps:

1. Open Active Directory Sites and Services, expand **Sites**, expand the site that contains the servers that you want to configure as preferred bridgehead servers, and then expand **Servers**.
2. Open the **Properties** dialog box for the server object that you want to become a preferred bridgehead server.
3. Select the IP or SMTP transport and then click **Add**.

Note For more information about the registry entries and configuration entries in Active Directory that are needed to adjust replication, see appendix A "Adjusting Replication" on the Student Materials compact disc.

Lab C: Monitoring Replication

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will monitor replication by using Replication Monitor and the **repadmin** utility.



*****ILLEGAL FOR NON-TRAINER USE*****

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Monitor replication by using Replication Monitor.
- Monitor replication by using the **repadmin** utility.

Lab Setup

To complete this lab, you need the Windows 2000 Advanced Server compact disc to install the Windows 2000 Support Tools.

Estimated time to complete this lab: 15 minutes

Exercise 1

Using Support Tools to Monitor Replication

Scenario

You have just finished the installation and configuration of a replica domain controller for a child domain of the Northwind Traders forest root domain. The domain controller's replication configuration needs to be verified to ensure replication is working properly.

Goal

In this exercise, you will use Replication Monitor to determine the replication directory partitions for your domain controller. You will also view your replication topology and server properties. You will then use the **repadmin** utility to view detailed information about your replication partners.

Tasks	Detailed Steps
1. Install (if not already installed) the Windows 2000 Support Tools with all of the default options.	- Log on as Administrator in your domain with a password of password. - If the Windows 2000 Support Tools have not already been installed, from your Windows 2000 Advanced Server compact disc, under the Support/Tools folder, run Setup to start the Windows 2000 Support Tools Setup wizard. - On the Welcome to the Windows 2000 Support Tools Setup Wizard page, click Next to continue. - On the User Information page, type your name in the Name box, type your organization in the Organization box, and then click Next. - On the Select An Installation Type page, ensure that Typical is selected and then click Next. - On the Begin Installation page, click Next to begin the installation of the Windows 2000 Support Tools.  <i>The wizard takes a short time to complete the installation.</i> - On the Completing the Windows 2000 Support Tools Setup Wizard page, click Finish.
2. Identify the replication directory partitions for your domain controller by using Active Directory Replication Monitor.	- Click Start, point to Programs, point to Windows 2000 Support Tools, point to Tools, and then click Active Directory Replication Monitor. - On the Edit menu, click Add Monitored Server. - In the Add Server to Monitor dialog box, click Add the server explicitly by name, and then click Next. - In the Enter the name of the server to monitor explicitly box, type <i>servername</i> (where <i>servername</i> is the host name of your computer) and then click Finish.

Tasks	Detailed Steps
 Using the information from Active Directory Replication Monitor, list the directory partitions that are replicated to your domain controller. CN=Schema,CN=Configuration,DC=nwtraders,DC=msft CN=Configuration,DC=nwtraders,DC=msft DC=<i>domain</i>,DC=nwtraders,DC=msft (where <i>domain</i> is your assigned domain name)	
2. (continued)	e. Expand each replication directory partition, and then examine the replication partners for each partition. Note: An icon with two connected computers indicates a direct partner. An icon with a single computer indicates a transitive partner.
3. View your replication topology by using Active Directory Replication Monitor.	a. In Active Directory Replication Monitor, right-click <i>servername</i>, and then click Show Replication Topologies. b. In the View Replication Topology window, on the View menu, click Connections Objects Only. c. Right-click the <i>servername</i> icon, and then click Show Intra-Site Connections.  <i>The lines drawn to your domain controller represent your inbound connections.</i> d. Close the View Replication Topology window.
4. View the configuration of your domain controller by using Active Directory Replication Monitor.	a. In Replication Monitor, right-click <i>servername</i>, and then click Properties. b. In the Server Properties dialog box, click the Server Flags tab.  <i>The properties with a check indicate the feature is enabled. An 'X' instead of a check indicates the domain controller does not have that feature enabled.</i> c. In the Server Properties dialog box, click the FSMO Roles tab.  <i>The listing displayed is the operations master role holders as known by this domain controller.</i> d. In the Server Properties dialog box, click the Inbound Replication Connections tab. Scroll through the description of why the connection objects were established. Click OK to close the Server Properties dialog box. e. Close Active Directory Replication Monitor.

Tasks	Detailed Steps
5. View the detailed configuration of your replication partners using repadmin , and then log off.	- Open a command prompt window. - At the command prompt, type repadmin /? to display its usage, and then review the usage for the /showreps option. - At the command prompt, type repadmin /showreps and then press ENTER to display details for inbound neighbors and outbound neighbors for change notification.
 Use the information from repadmin to determine when the last schema directory partition replication was made and why it was made. The schema and all directory partitions should have been replicated no more than one hour ago. This replication most likely did not occur because of an actual change in the schema, but rather because of the one hour scheduled replication cycle.	
5. <i>(continued)</i>	Close the command prompt window, close all other open windows, and then log off.

Troubleshooting Active Directory Replication

Topic Objective

To troubleshoot common problems with Active Directory replication.

Lead-in

You may encounter problems related to replication in Active Directory. Most problems can be remedied with Active Directory Sites and Services.



Replication Does Not Finish



Replication Is Slow



Replication Increases Network Traffic



Replication Clients Are Receiving a Slow Response



KCC Was Unable to Complete the Topology

*****ILLEGAL FOR NON-TRAINER USE*****

Ineffective replication can result in Active Directory not functioning properly, such as new user accounts not being recognized, outdated directory information, or unavailable domain controllers. You may encounter problems related to replication in Active Directory. Most problems can be remedied with Active Directory Sites and Services. Some of the common problems are:

- Replication does not finish. The possible cause could be that the sites containing the client computers and domain controllers are not connected by site links to domain controllers in other sites in the network. This results in a failure to exchange directory information between sites. To overcome this problem, create a site link from the current site to a site that is connected to the rest of the sites in the network.
- Replication is slow. The possible cause is that the topology and schedule of the site links cause the replication of information to go through many sites serially before all sites are updated. For example, site A can communicate with site B on Monday, site B can communicate with site C on Saturday. A change originating in Site A on Tuesday will not be given to Site C until a week from Saturday.
- Replication increases network traffic. The possible problem could be that the current network resources are insufficient to handle the amount of replication traffic. This problem can also affect services unrelated to Active Directory, because the exchange of information in Active Directory is consuming an inordinate amount of network resources. To solve this problem, you can use sites and schedule the replication to occur during off-peak hours when there is more network bandwidth available for replication.

- Replication clients are receiving a slow response for authentication, directory information, or other services. The possible cause could be that the client computers must request authentication, information, and services from a domain controller through a low-bandwidth connection. If there is a site that serves a client computer's subnet well, associate that subnet with the site. If a client computer that is experiencing slow response for services is isolated from domain controllers, and you plan to create another site that includes the client computer, create a new site with its own domain controller. You can also install a connection with more bandwidth.
- KCC was unable to complete the topology for the distinguished name of the site. If this message appears in the Directory Service log in Event Viewer, it indicates that there is an exception in the KCC. To log more information, increase the value of the **9 Internal Processing** registry entry and **1 Knowledge Consistency Checker** registry entry to three and wait 15 minutes. The registry entries are at the location: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics**. Alternatively, you can also run **repadmin /kcc**, and reset the value of the registry entry to 0. By default, only the most important events are logged in KCC. You can increase the level of detail by modifying the value in the **Replication Events** entry in an event log.

Best Practices

Topic Objective

To list best practices for managing Active Directory replication.

Lead-in

Review this checklist before you manage replication in Active Directory.



Place at Least One Domain Controller in Every Site



Place At Least One DNS Server in Each Site



Schedule Site Links for Times When Network Traffic Is Slow

*****ILLEGAL FOR NON-TRAINER USE*****

Emphasize the reason for each best practice.

The following list provides best practices for administering Active Directory:

- Place at least one domain controller in every site, and create a global catalog on at least one domain controller in each site. Sites that do not have their own domain controllers and at least one global catalog are dependent on other sites for directory information, making the usage of network bandwidth between sites less efficient. Also, placing a domain controller in every site and a global catalog on the domain controller in each site can make the site less susceptible to WAN failures.
- Place at least one Domain Name System (DNS) server in each site. Sites that do not have their own DNS server are dependent on other sites for name resolution information, making the usage of network bandwidth between sites less efficient. Also, placing a DNS server in every site can make the site less susceptible to WAN failures.
- Schedule site links for times when network traffic is slow. This type of scheduling reduces the replication traffic on the network.

Review

Topic Objective

To reinforce module objectives by reviewing key points.

Lead-in

The review questions cover some of the key concepts taught in the module.

- Introduction to Active Directory Replication
- Replication Components and Processes
- Replication Topology
- Using Sites to Optimize Active Directory Replication
- Implementing Sites to Manage Active Directory Replication
- Monitoring Replication Traffic
- Adjusting Replication
- Troubleshooting Active Directory Replication
- Best Practices

*****ILLEGAL FOR NON-TRAINER USE*****

Give students time to read and answer the review questions on their own, and then discuss the answers as a group.

1. All domain controllers in replication are connected in a loop. Therefore, during replication, updates can be replicated to domain controllers more than once. How does Active Directory prevent this from happening?

It uses the up-to-dateness vector of propagation dampening.

2. An administrator changes the telephone number on a user object in Active Directory on one domain controller. A short time later, the user changes his pager number on another domain controller. What happens to the two changes when they are replicated to domain controllers throughout the domain?

Both attribute changes are replicated to all domain controllers. Because different attributes were updated, and replication is maintained at the attribute level, no conflict occurs.

3. When you observe your Active Directory replication topology on your network, you notice that one of your most capable servers is not the bridgehead server. What can you do to make this server a bridgehead?

Configure this server as a preferred bridgehead server.

4. You want to limit the replication traffic between two domain controllers connected by a WAN link. You also want this link to be used only for replication traffic at night. What should you do?

Put the domain controllers in separate sites, and create a site link between them with a replication scheduled to occur only at night.

5. To reduce congestion on your network, the Network Services group in your organization has created a new high-speed backbone on a separate IP subnet for servers in your location. What should you do before you move your domain controllers to the new backbone?

Associate the backbone's subnet with a site.

6. Which utility allows you to view the status of replication on domain controllers in the domain?

The Repadmin.exe utility or Replication Monitor.