
Module 12: Managing Operations Masters

Contents

Overview	1
Introduction to Operations Masters	2
Operations Master Roles	3
Managing Operations Master Roles	12
Managing Operations Master Failures	21
Lab A: Managing Operations Masters	24
Best Practices	34
Review	35
Course Evaluation	37



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:
45 Minutes

This module provides students with the knowledge and skills to manage operations masters.

Lab:
45 Minutes

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

- Define an operations master and describe its importance in an Active Directory® directory service network.
- Describe the functions of each of the five operations master roles in a forest.
- Determine, transfer, and seize an operations master role.
- Describe the effects of, and how to respond to, an operations master failure.
- Apply best practices for managing an operations master.

In the hands-on lab in this module, students will have the opportunity to manage operations master roles.

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_12.ppt

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the lab.
- Study the review questions and prepare alternative answers to discuss.
- Anticipate questions that students may ask. Write out the questions and provide the answers.

Module Strategy

Use the following strategy to present this module:

- Introduction to Operations Masters

In this topic, you will introduce operations masters. Explain the use of an operations master in Active Directory. Emphasize that operations masters perform updates to the forest that should not be performed as multi-master updates. Clarify that any domain controller can be an operations master, and that it is possible to move an operations master role from one domain controller to another.

- Operations Master Roles

In this topic, you will introduce the operations master roles. Begin with introducing the five types of operations master roles and their default locations in Active Directory. Describe the functions of each of the five operations master roles: schema master, domain naming master, primary domain controller (PDC) emulator, relative identifier (RID) master, and infrastructure master.

- Managing Operations Master Roles

In this topic, you will introduce managing operations master roles. Begin by explaining how to determine the holder of an operations master role. Reinforce that the tool used to determine a specific operations master role is related to whether the scope of the operations master is domain wide or forest wide. Next, describe the procedure for transferring an operations master role. Finally, explain how to seize an operations master role. Emphasize that the same Active Directory snap-in is used to seize or transfer an operations master role as is used to determine the role.

- Managing Operations Master Failures

In this topic, you will introduce managing operations master failures. Explain how to manage a failure of the PDC emulator and infrastructure master roles. Emphasize that the loss of the PDC emulator role can affect the usability of the network, and the administrator should seize the PDC emulator role if it is known that the current PDC emulator will be unavailable for a long time. Also, explain how to manage the failure of other operations master roles.

- Lab A: Managing Operations Masters

Prepare students for the lab in which they will manage operations master roles. Tell students that they will work in pairs for this lab. Students will determine the role of each operations master, transfer an operations master role from one domain controller to another, and seize an operations master role from a failed domain controller. They will also use the **ntdsutil** utility to manage operations masters. After students have completed the lab, ask them if they have any questions concerning the lab.

- Best Practices

Present best practices for managing operations masters. 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 on 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).
 - 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\Autode 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:

- The Active Directory Schema snap-in is registered.
- The infrastructure master and RID master roles are transferred to the second domain controller in each child domain.

Overview

Topic Objective

To provide an overview of the module topics and objectives.

Lead-in

In this module, you will learn about the types of operations masters used in Active Directory and how to manage them.

- Introduction to Operations Masters
- Operations Master Roles
- Managing Operations Master Roles
- Managing Operations Master Failures
- Best Practices

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

An *operations master* is a domain controller that performs a specific role in Microsoft® Windows® 2000 Active Directory® directory service and may control a specific set of directory changes. For each role, only the domain controller holding that role can make the associated directory changes. There are ways to move these roles from one domain controller to another, even if an operations master fails. Knowing the specific operations master roles that each domain controller holds in an Active Directory network can help you take advantage of data replication and network bandwidth.

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

- Define an operations master, and describe its importance in an Active Directory network.
- Describe the functions of each of the five operations master roles in a forest.
- Determine, transfer, and seize an operations master role.
- Describe the effects of, and how to respond to, an operations master failure.
- Apply best practices for managing an operations master.

Introduction to Operations Masters

Topic Objective

To introduce the use of an operations master in Active Directory.

Lead-in

There are situations in which a single master update of a forest is required instead of the usual multi-master update.

- Only a Domain Controller That Holds a Specific Operations Master Role Can Perform Associated Active Directory Changes
- Changes Made by an Operations Master Are Replicated to Other Domain Controllers
- Any Domain Controller Can Hold an Operations Master Role
- Operations Master Roles Can Be Moved to Other Domain Controllers

Single Master Operations

Operations Master

Replication

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

Key Points

Operations masters perform updates to the forest that should not be performed as multi-master updates.

Any domain controller can be an operations master.

It is possible to move an operations master role to other domain controllers.

Active Directory supports multi-master replication of directory changes among all domain controllers in a forest. During multi-master replication, a replication conflict can potentially occur if concurrent originating updates are performed on the same data on two different domain controllers.

To avoid these conflicts, some operations are performed in *single master* (not permitted to occur at different places in the network at the same time) fashion by making a single domain controller responsible for the operation. These operations are grouped together into specific roles within the forest or within a domain. These roles are called *operations master roles*. For each operations master role, only the domain controller holding that role can make the associated directory changes. The domain controller responsible for a particular role is called an *operations master* for that role.

Active Directory stores information about which domain controller holds a specific role. Clients that can query Active Directory use this information to contact an operations master when necessary. Any domain controller can potentially be configured as an operations master. It is possible to move an operations master role to other domain controllers, even when the current operations master role holder is unavailable.

◆ Operations Master Roles

Topic Objective

To introduce the operations master roles unique to a domain and a forest.

Lead-in

There are five different operations master roles. These roles are unique to either a domain or a forest.

- **Operations Master Default Locations**
- **Schema Master**
- **Domain Naming Master**
- **PDC Emulator**
- **RID Master**
- **Infrastructure Master**

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

Emphasize domain wide vs. forest wide roles.

Active Directory defines five operations master roles, each one of which has a default location. The five operations master roles are:

- Schema master
- Domain naming master
- Primary domain controller (PDC) emulator
- Relative identifier (RID) master
- Infrastructure master

The schema master and domain naming master are per-forest roles, meaning that there is only one schema master and one domain naming master in the entire forest. The other operations master roles are per-domain roles, meaning that each domain in the forest has its own PDC emulator, RID master, and infrastructure master. So, in a forest with only one domain, there are five operations master roles. In a forest with more than one domain, there are more than five roles because the per-domain roles need to exist in each domain.

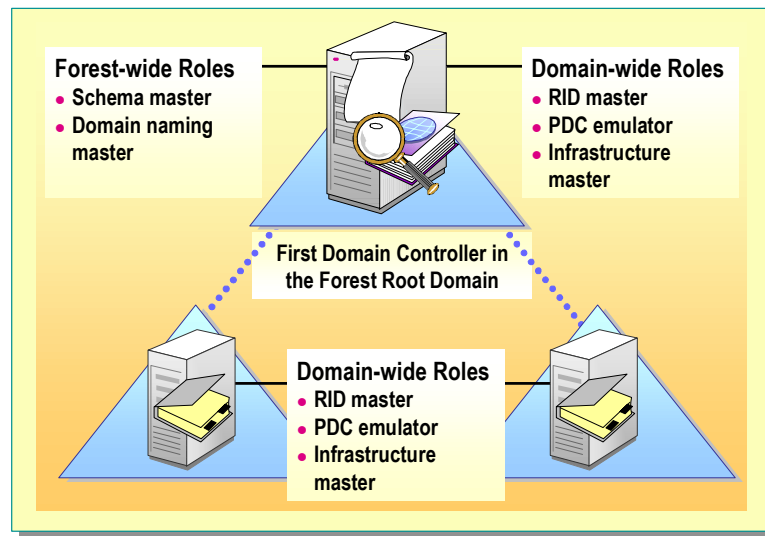
Operations Master Default Locations

Topic Objective

To illustrate the default locations of Active Directory operations master role holders.

Lead-in

There are two forest-wide operations master roles and three domain-wide operations master roles.



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

Delivery Tips

Use the graphic on the slide to illustrate the default locations of forest-wide and domain-wide operations master role holders.

Key Points

The first domain controller of a new forest holds all five operations master roles and is also a global catalog server.

The first domain controller for each new domain joining an existing forest holds the three domain operations master roles for the new domain.

Operations master roles are either forest wide or domain wide.

- Forest-wide roles are unique for a forest. The schema master and the domain naming master are forest-wide roles. This means that there is only one schema master and one domain naming master in the entire forest.
- Domain-wide roles are unique for each domain in a forest. The PDC emulator, the RID master, and the infrastructure master are domain-wide roles. This means that each domain in a forest has its own PDC emulator, RID master, and infrastructure master.

By default, the first domain controller of a new forest holds all five operations master roles. The first domain controller for each new domain joining an existing forest holds the three domain-wide operations master roles for the new domain.

As the network expands, the operations master placement would be as follows:

- In a forest with only one domain, there are five operations master roles.
- In a forest with more than one domain, there are two per-forest operations master roles. The three per-domain operations master roles are duplicated for each domain.

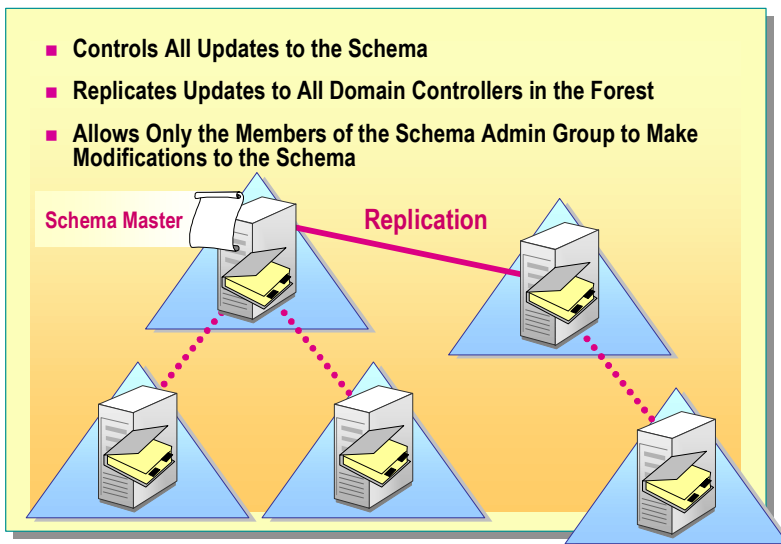
Schema Master

Topic Objective

To describe the function of the schema master.

Lead-in

The schema master controls all updates to the schema.



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

Key Points

The single forest-wide schema master performs all schema modifications, which are then replicated to all of the domain controllers in the forest.

The *schema master* controls all originating updates to the schema. The schema contains the master list of object classes and attributes that are used to create all Active Directory objects, such as computers, users, and printers. The domain controller that holds the schema master role is the only domain controller that can perform write operations to the directory schema. These schema updates are replicated from the schema operations master to all other domain controllers in the forest. Having only one schema master per forest prevents any conflicts that would result if two or more domain controllers attempt to concurrently update the schema. Only the Schema Admins group can make modifications to the schema.

Domain Naming Master

Topic Objective

To explain the function of the domain naming master.

Lead-in

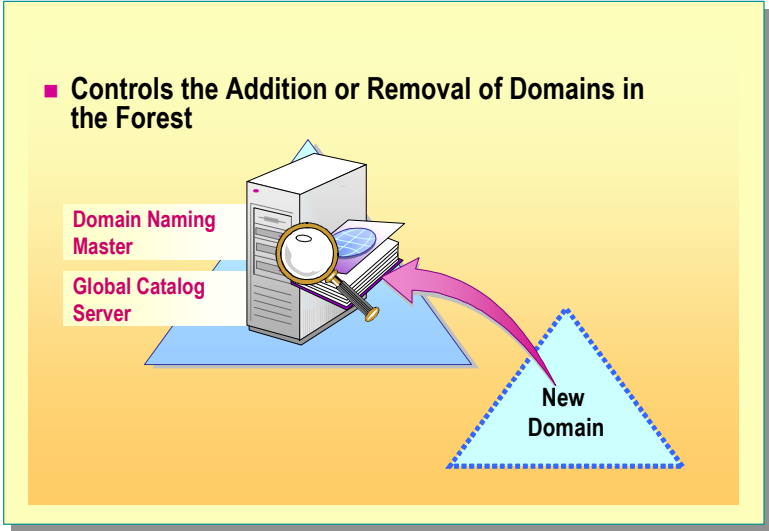
The domain naming operations master prevents multiple domains from joining the forest with the same domain name.

■ Controls the Addition or Removal of Domains in the Forest

Domain Naming Master

Global Catalog Server

New Domain



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

Key Points

Only the domain controller that holds the domain naming master role can add or remove new domains to the forest.

The domain naming master must also be a global catalog server because the domain naming master cannot query a separate domain controller that runs as a global catalog server.

The *domain naming master* controls the addition or removal of domains in the forest. There is only one domain naming master per forest.

When you add a new domain to the forest, only the domain controller holding the domain naming master role has the right to add the new domain. The domain naming master manages this process, preventing multiple domains from joining the forest with the same domain name. When you use the Active Directory Installation wizard to create a child domain, it contacts the domain naming master and requests the addition or deletion. The domain naming master is responsible for ensuring that the domain names are unique. Note that if the domain naming master is unavailable, you cannot add or remove domains.

The domain controller holding the domain naming master role must also be a global catalog server. When the domain naming master creates an object that represents a new domain, it verifies by querying the global catalog server that no other object, including domain objects, is using the same name as the new object. Because the domain naming master verifies the name of a new object by querying the global catalog server, the global catalog must run on the same domain controller as the one holding the domain naming master role. The domain naming master also manages the naming of sites to ensure that a duplicate site is not created.

PDC Emulator

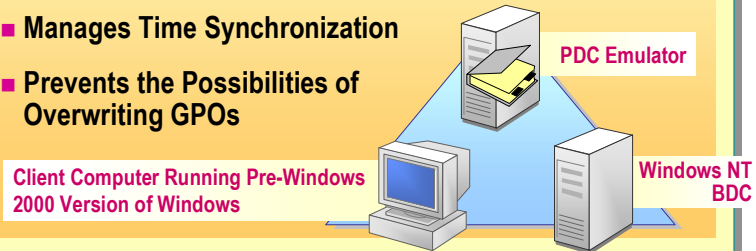
Topic Objective

To identify the function of the PDC emulator.

Lead-in

The PDC emulator acts as a primary domain controller for computers running Windows NT.

- Acts As a PDC to Support Windows NT BDCs and Pre-Windows 2000-based Client Computers
- Updates Password Changes from Pre-Windows 2000-based Client Computers
- Minimizes Replication Latency for Password Changes for Windows 2000-based Client Computers
- Manages Time Synchronization
- Prevents the Possibilities of Overwriting GPOs



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

If appropriate, briefly describe the function of Windows NT PDCs and BDCs.

Key Points

The *PDC emulator* acts as a Windows NT PDC in a mixed-mode domain.

The *PDC emulator* acts as a Microsoft Windows NT® PDC to support any backup domain controllers (BDCs) running Windows NT within a mixed-mode domain. The PDC emulator is the first domain controller that is created in a new domain.

The PDC emulator performs the following roles:

- Acts as the PDC for any existing BDCs.

If a domain contains any BDCs or client computers that are running pre-Windows 2000 versions of Windows, the PDC emulator functions as a Windows NT PDC. The PDC emulator services client computers and replicates directory changes to any BDCs running Windows NT.

- Manages password changes from computers running Windows NT, Windows 95, or Windows 98, which need to be written to the directory.
- Minimizes replication latency for password changes.

Replication latency is the time needed for a change made on one domain controller to be received by another domain controller. When the password of a client computer running Windows 2000 is changed on a domain controller, that domain controller immediately forwards the change to the PDC emulator. If a password was recently changed, that change takes time to replicate to every domain controller in the domain. If a logon authentication fails at another domain controller because of a bad password, that domain controller will forward the authentication request to the PDC emulator before rejecting the logon attempt.

- Synchronizes the time on all domain controllers throughout the domain to its time.

All domain controllers in the domain get their time synchronized to the clock of the PDC emulator of that domain. The PDC emulator of the domain gets its clock set to the PDC emulator's clock in the forest root domain. The forest root domain's PDC emulator should be configured to synchronize with an external time source. The end result is that the time kept by the clocks of all Windows 2000-based computers in the entire forest is within seconds of each other.

Note Only when the domain is in mixed mode does the domain controller that holds the PDC emulator role synchronize with BDCs running Windows NT versions 4.0 or 3.51.

- Prevents the possibilities of overwriting Group Policy objects (GPOs).

The Group Policy snap-in, by default, runs on the domain controller that holds the PDC emulator role for that domain. This is done to reduce the potential for replication conflicts. It is not a requirement, however that a Group Policy object (GPO) be updated on this domain controller.

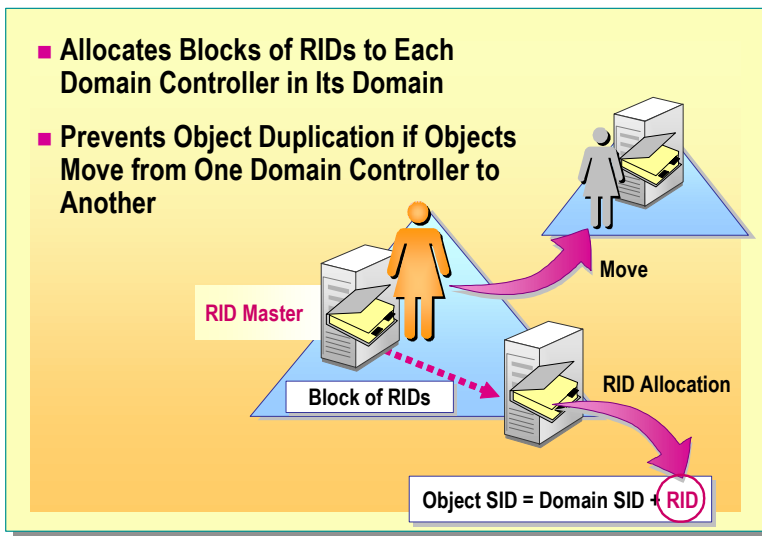
RID Master

Topic Objective

To explain the functions of the RID master.

Lead-in

The RID master ensures that all domain SIDs are unique by allocating blocks of RIDs to domain controllers when they need them.



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

Key Points

The RID is unique for each object.

The RID master manages the RID creation when an object is created or moved.

The *relative identifier (RID) master* allocates blocks of RIDs to each domain controller in the domain. Whenever a domain controller creates a new security principal, such as a user, group, or computer object, it assigns the object a unique security identifier (SID). This SID consists of a domain SID, which is the same for all security principals created in the domain, and a RID, which is unique for each security principal created in the domain.

The RID master supports creating and moving objects as follows:

- **Creating objects.** To allow a multi-master operation to create objects on any domain, the RID master allocates a block of RIDs to a domain controller. When a domain controller needs an additional block of RIDs, it initiates communication with the RID master. The RID master allocates a new block of RIDs to the domain controller, which the domain controller assigns to the new objects.

The process of creating the objects and communicating to the RID master for additional blocks of RIDs can be repeated as many times as necessary. If a domain controller's RID pool is empty, and the RID master is unavailable, new security principals cannot be created on that domain controller. You can view the RID pool allocation by using the **dcdiag** utility.

- **Moving objects.** When you move an object between domains, you must initiate the move on the RID master that currently contains the object. This prevents the possible duplication of objects. If an object were moved, but there were no single master that kept this information, then it would be possible to move the object to multiple domains without realizing that a previous move had already taken place.

The RID master deletes the object from the domain when the object is moved from that domain to another domain.

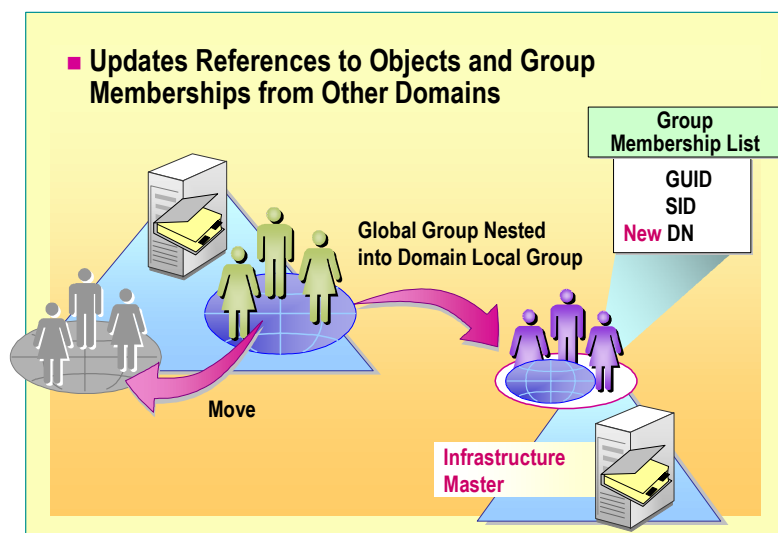
Infrastructure Master

Topic Objective

To illustrate the function of the infrastructure master.

Lead-in

The infrastructure master is responsible for updating group membership data for groups that have members that move between two or more domains.



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

Key Points

The infrastructure master is responsible for updating the external references to an object whenever the object changes.

The infrastructure master compares its data with that of a global catalog server.

The infrastructure master should not be the same computer that hosts a global catalog in a multiple domain forest.

The *infrastructure master* is used to update object references in its domain that point to the object in another domain. The object reference contains the object's globally unique identifier (GUID), distinguished name and possibly a SID. The distinguished name and SID on the object reference are periodically updated to reflect changes made to the actual object. These changes include moves within and between domains as well as the deletion of the object.

Group Membership Identification

If SID or distinguished name modifications to user accounts and groups are made in other domains, the group membership for a group on your domain that references the changed user or group needs to be updated. The infrastructure master for the domain in which the group (or reference) resides is responsible for this update; it distributes the update through normal replication throughout its domain.

The infrastructure master updates object identification, by the following rules:

- If the object moves at all, its distinguished name will change because the distinguished name represents its exact location in the directory.
- If the object is moved within the domain, its SID remains the same.
- If the object is moved to another domain, the SID changes to incorporate the new domain SID.
- The GUID does not change regardless of location (the GUID is unique across domains).

Note In a single domain forest, the infrastructure master does not need to function because there are no external object references for it to update.

Infrastructure Master and the Global Catalog

The infrastructure operations master should not be the same domain controller that hosts the global catalog. If the infrastructure master and the global catalog are the same computer, the infrastructure master will not function because it does not contain any references to objects that it does not hold. In this case, the domain replica data and the global catalog server data cannot exist on the same domain controller.

The infrastructure master for a domain periodically examines the references, within its replica of the directory data, to objects not held on that domain controller. It queries a global catalog server for current information about the distinguished name and SID of each referenced object. If this information has changed, the infrastructure master makes the change in its local replica. These changes are replicated using normal replication to the other domain controllers within the domain.

◆ Managing Operations Master Roles

Topic Objective

To introduce the methods of managing operations master roles.

Lead-in

There are tasks you need to perform during network administration to manage operations masters.

- **Determining the Holder of an Operations Master Role**
- **Transferring an Operations Master Role**
- **Seizing an Operations Master Role**

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

When you create a Windows 2000 domain, Windows 2000 automatically configures all of the operations master roles. However, it may be necessary to reassign an operations master role to another domain controller in the forest or in the domain. To reassign an operations master role to another domain controller:

- Determine the holder of the operations master role.
- Transfer the operations master role.
- Seize the operations master role.

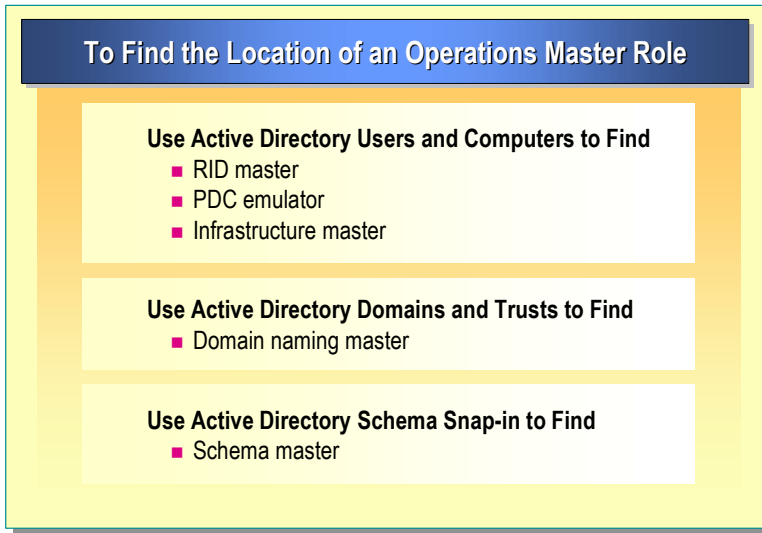
Determining the Holder of an Operations Master Role

Topic Objective

To explain how to verify which domain controller is the holder of a given operations master role.

Lead-in

Before you manage the operations master, you should verify that the operations master role has a domain controller assigned.



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

Demonstrate the steps to determine the different operations master roles.

Reinforce the concept that the tool used to determine a specific operations master is related to whether the scope of the operations master is domain wide or forest wide.

Before you consider moving an operations master role, you may need to determine which domain controller holds a specific operations master role. Authenticated Users have the permission to determine where the operations master roles are located. Depending on the operations master role to be determined, you use one of the following Active Directory consoles:

- Active Directory Users and Computers
- Active Directory Domains and Trusts
- Active Directory Schema

Determining the RID Master, the PDC Emulator, and the Infrastructure Master

To determine which domain controller holds the RID master, PDC emulator, or infrastructure master roles, perform the following steps.

1. Open Active Directory Users and Computers.
2. In the console tree, right-click **Active Directory Users and Computers**, and then click **Operations Masters**.
3. Click the **RID**, **PDC**, or **Infrastructure** tab.

The name of the current operations master appears under **Operations master**.

Determining the Domain Naming Master

To determine which domain controller holds the domain naming master role, perform the following steps:

1. Open Active Directory Domains and Trusts.
2. Right-click **Active Directory Domains and Trusts**, and then click **Operations Master**.

The name of the current domain naming master appears in the **Change Operations Master** dialog box.

Determining the Schema Master

To determine which domain controller holds the schema master role, perform the following steps:

1. Register the Active Directory Schema snap-in by running the following command:
regsvr32.exe %systemroot%\system32\schmmgmt.dll
2. Click **OK** to close the message that indicates the registration succeeded.
3. Create a custom Microsoft Management Console (MMC) console.
4. Add the Active Directory Schema snap-in to the console.
5. In the console tree, right-click **Active Directory Schema**, and then click **Operations Master**.

The name of the current schema master appears in the **Change Schema Master** dialog box.

Note To identify an operations master in a different domain, connect to the domain before clicking **Operations Masters**. To identify the operations master in a different forest, connect to the domain by typing the domain name of the forest before clicking **Operations Masters**.

Transferring an Operations Master Role

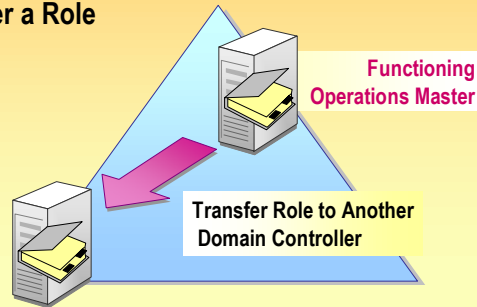
Objective

To illustrate how to transfer an operations master role to a different domain controller.

Lead-in

Transferring an operations master role means moving it from one domain controller to another.

- **Transfer Roles Only When Making a Major Change to the Domain Infrastructure**
- **No Loss of Data**
- **You Must Be a Member of an Authorized Group To Transfer a Role**



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

Demonstrate the steps to transfer the different operations master roles.

Tell the class that a one-time registration of the Active Directory schema snap-in is necessary before opening the Active Directory schema.

Key Points

To transfer an operations master role, use the same Active Directory snap-in that you used to determine the operations master role.

In most cases, the placement of operations master roles in a forest does not require changes as the forest grows, which means that role placements do not require revisions. However, when you plan to decommission a domain controller, reduce the connectivity of your network, or change the global catalog server status of a domain controller, you need to review your plan and transfer operations master roles as necessary. Transferring an operations master role means moving it from one functioning domain controller to another. To transfer roles, both domain controllers must be up and running and connected to the network.

There is no loss of data during a role transfer. The process of role transfer involves replicating the current operations master directory to the new domain controller, which ensures that the new operations master has the most current information available. This transfer of the role object uses the normal directory replication mechanism.

To transfer an operations master role, you must have the appropriate permissions to do so. The following table lists the groups of which you must be a member to have permissions to change an operations master role.

Operations master	Authorized group
Schema master	The Change Schema Master permission is granted by default to the Schema Admins group.
Domain naming master	The Change Domain Master permission is granted by default to the Enterprise Admins group.
PDC emulator	The Change PDC permission is granted by default to the Domain Admins group.
RID master	The Change Rid Master permission is granted by default to the Domain Admins group.
Infrastructure master	The Change Infrastructure Master permission is granted by default to the Domain Admins group.

Important Transfer roles only when making a major change to the domain infrastructure, such as decommissioning a domain controller that holds a role or adding a new domain controller that is better suited to hold a specific role.

Note When a domain controller is demoted to a member server, all operations master roles are relinquished to other domain controllers. To control the transfer of roles to the other domain controllers, transfer the roles prior to demotion.

To transfer an operations master role, use the same Active Directory snap-in that you use to determine the operations master role.

Transferring the RID Master, PDC Emulator, and Infrastructure Master Roles

To transfer the operations master role for the RID master, PDC emulator, or infrastructure master, perform the following steps:

1. Open Active Directory Users and Computers.
2. In the console tree, right-click **Active Directory Users and Computers**, and then click **Connect to Domain Controller**.
3. In the list of available domain controllers, click the domain controller that will become the new operations master, and then click **OK**.
4. In the console tree, right-click the icon of the domain controller that will become the new operations master, and then click **Operations Masters**.
5. Click the tab for the operations master role you want to transfer, such as PDC, and then click **Change**.

Caution Ensure that you do not transfer the infrastructure master role to a domain controller that hosts the global catalog.

Transferring the Domain Naming Master Role

To transfer the domain naming master role to another global catalog server, perform the following steps:

1. Open Active Directory Domains and Trusts.
2. In the console tree, right-click **Active Directory Domains and Trusts**, and then click **Connect to Domain Controller**.
3. In the list of available domain controllers, click the domain controller that will become the new domain naming master, and then click **OK**.
4. In the console tree, right-click **Active Directory Domains and Trusts**, and then click **Operations Master**.
5. The name of the domain controller you selected appears.
6. Click **Change**.

Note Ensure that the domain controller that holds the domain naming master role also hosts the global catalog.

Transferring the Schema Master Role

To transfer the schema operations master role, perform the following steps:

1. Open Active Directory Schema.
2. In the console tree, right-click **Active Directory Schema**, and then click **Change Domain Controller**.
3. Click **Specify Name**, type the name of the domain controller to which you want to transfer the schema master role, and then click **OK**.
4. In the console tree, right-click **Active Directory Schema**, and then click **Operations Master**.
5. The name of the domain controller you selected appears.
6. Click **Change**.

Note You need to register the schema admin snap-in, Schmgmt.dll, before opening the Active Directory schema.

Seizing an Operations Master Role

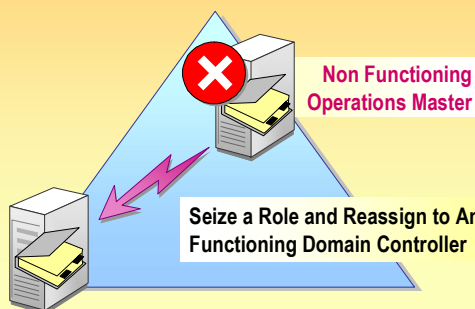
Topic Objective

To illustrate how to seize an operations master role from a failed domain controller.

Lead-in

If a domain controller that holds an operations master role becomes unavailable, it may become necessary to seize the operations master role and reassign it to another domain controller.

- **Seize Roles Only When There Is the Potential for Loss of Network Services**
- **Possible Loss of Data**
- **You Must Be a Member of an Authorized Group to Seize a Role**



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

Demonstrate the steps to seize the different operations master roles.

For **ntdsutil**, tell students that they can type **help** at any prompt to display help information about the commands that can be used at a specific prompt.

Key Points

Seizing an operations master role is a major step that should be considered only if the current operations master will never be available again.

Before seizing an operations master role, you must permanently disconnect the current operations master from the network.

To seize an operations master role, use the same Active Directory snap-in that you use to determine or transfer the operations master role.

Seizing an operations master role means forcing a transfer of an operations master role from a domain controller that has failed to a functioning domain controller.

Seizing an operations master role is a drastic step that you should consider only if the current operations master will never be available again. If the cause of the failure is a networking problem or a software or hardware failure that you can resolve in a timely manner, wait for the operations master role holder to become available again. You should seize a role only if it cannot be transferred. Unlike role seizure, a role transfer ensures that only one domain controller holds the role, and that the role holder has an updated role object set.

Important Before proceeding with the role seizure, you must permanently disconnect from the network the domain controller that currently holds the operations master role.

Before you seize an operations master role, you should determine which domain controller holds the operations master role. After you determine the current role holder, seize the operations master role by using either the Active Directory console you used for determining or transferring a role, or the **ntdsutil** command. Finally, verify that the functioning domain controller has accepted its new operations master role.

Seizing the PDC Emulator and Infrastructure Master Roles

To seize an operations master role for the PDC emulator or infrastructure master, perform the following steps:

1. Open Active Directory Users and Computers.
2. In the console tree, right-click **Active Directory Users and Computers**, and then click **Operations Masters**.

Note It may take some time for the data to display because it is waiting for a response from the current holder of the operations master role. Because the current role holder has failed and cannot respond, the last updated information appears.

3. In the **Operations Master** dialog box, click the tab of the operations master role you want to seize.
4. Click **Change**, and when the message appears indicating a transfer is not possible, click **Yes** in the confirmation dialog box.
5. Click **OK** on the warning page, and then click **OK** to perform a forceful transfer.
6. Click **OK** to close the **Operations Master** dialog box.
7. Verify the new holder of the operations master role that you seized.

Seizing Other Operations Master Roles

Temporary loss of the schema master, domain naming master, or RID master is ordinarily not visible to end users, and does not usually inhibit your work as an administrator. Therefore, this is usually not a problem worth fixing. However, if you anticipate an extremely long outage of the domain controller holding one of these roles, you can seize that role to the standby operations master domain controller. But seizing any of these roles is a step that you would take only when the outage is permanent, as in the case when a domain controller is physically destroyed and cannot be restored from backup media.

An operations master that has its role seized should not become operational because of the possibility of having multiple operations masters online for the same role. Before seizing the role, you must ensure that the outage of this domain controller is permanent by physically disconnecting the domain controller from the network.

Using Ntdsutil to Seize a Role

To use the **ntdsutil** command to seize an operations master role, perform the following steps:

1. In the **Run** box, type **cmd** and then press ENTER.
2. At the command prompt, type **ntdsutil**
3. At the **ntdsutil** prompt, type **roles**
4. At the **fsmo maintenance** prompt, type **connections**
5. At the **server connections** prompt, type **connect to server** followed by the fully qualified domain name (FQDN) of the domain controller that will be the new role holder.

6. At the **server connections** prompt, type **quit**
7. At the **fsmo maintenance** prompt, type one of the following commands to seize the appropriate operations master:
 - **Seize RID master**
 - **Seize PDC**
 - **Seize infrastructure master**
 - **Seize domain naming master**
 - **Seize schema master**
8. At the **fsmo maintenance** prompt, type **quit**
9. At the **ntdsutil** prompt, type **quit**
10. Verify the new holder of the operations master role that you seized.

◆ Managing Operations Master Failures

Topic Objective

To introduce the topics related to managing the failure of an operations master.

Lead-in

Some of the operations master roles are crucial to the operation of the network. Other operations master roles can be unavailable for quite some time before their absence becomes a problem.

- **Failure of the PDC Emulator or the Infrastructure Master**
- **Failure of Other Operations Masters**

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

The effects of a failure of an operations master on the network depend on the role of the operations master. Some of the operations master roles are crucial to the operation of the network, whereas others can be unavailable for quite some time before their absence becomes a problem. You will notice that an operations master is unavailable when you try to perform some function controlled by the particular operations master.

If the cause is a networking problem or a server failure, and the problem will be resolved soon, wait for the operations master to become available again. If the domain controller that currently holds the operations master role has failed, you must determine if it can be recovered and brought back online.

Generally, you want to seize the role of the failed operations master to prevent long-term network failure. For the PDC emulator and infrastructure operations master roles, it is safer to perform a seizure than for the other operations master roles.

Failure of the PDC Emulator or the Infrastructure Master

Topic Objective

To identify what to do in case of a failure of the PDC emulator or the infrastructure master.

Lead-in

The loss of the PDC emulator affects network users. Therefore, when the PDC emulator is not available, immediately seize the role.

- **Failure of the PDC Emulator Seriously Affects Network Operations**
- **Failure of the Infrastructure Master Is Not Serious Unless Operations Are Down for a Long Time**

To Recover From Failure

- 1 Determine which domain controller holds the operations master role**
- 2 Determine the severity of the problem with the domain controller**
- 3 Seize the operations master role and reassign it to another domain controller**
- 4 Verify that the new domain controller has accepted the operations master role**

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

Key Points

Because the loss of the PDC emulator role can affect the usability of the network, you should seize the PDC emulator role when you know that the current PDC emulator will be unavailable for a long time.

The failure of the PDC emulator may more seriously affect network users than the failure of other operations master roles because the PDC emulator is a role holder for more common network operations.

PDC Emulator Failure

Failure of the PDC emulator causes:

- Loss of support of client computers running pre-Windows 2000 versions of Windows for password changes.
- Loss of latency reduction for password updates.
- Possible loss of time synchronization among domain controllers.

Infrastructure Master Failure

Temporary failure of the infrastructure operations master is not as serious as failure of the PDC emulator. End users may not notice that it is not functioning. Its role has minimal impact unless you move a large number of objects.

If the infrastructure master will be unavailable for a long time, seize the role and give it to a domain controller that is not a global catalog server. When the original domain controller returns to service, you may or may not transfer the infrastructure role back to the original domain controller.

Managing PDC Emulator or Infrastructure Master Failure

To recover from a failure of the PDC emulator and infrastructure master, perform the following steps:

1. Determine which domain controller holds the operations role.
2. Determine the severity of the problem with the domain controller.
3. Seize the operations master role and give it to another domain controller. In the case of the infrastructure master, make sure that the receiving domain controller it is not a global catalog server.
4. Verify that the new domain controller has accepted the operations master role.

Failure of Other Operations Masters

Topic Objective

To identify what to do in the case of failure of an operations master other than the PDC emulator and the infrastructure operations master.

Lead-in

Seizing should be considered a drastic measure for roles other than the PDC emulator and infrastructure operations masters.

To Recover from Other Operations Master Failures

- 1** Permanently disconnect the current operations master from the network
- 2** Wait until all updates made by the failed domain controller have been replicated to the domain controller seizing the role
- 3** Ensure that the domain controller whose role was seized is never restored
- 4** Reformat the partition that contained the operating system files of the original operations master and reinstall Windows 2000 before reconnecting that computer to the network

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

Temporary unavailability of the schema master, RID master, and domain naming master roles is not immediately visible to network users. When possible, it is best to transfer or restore these operations master roles from backup instead of seizing the role because there is always a possibility of replication errors in the data. Consider seizing the role of these operations masters only when all other options are exhausted.

If you must recover from an RID master, schema master, or domain naming master failure, use the following guidelines:

1. Disconnect the current operations master from the network before proceeding with the role seizure. To perform the seizure, use the **ntdsutil** command.
2. Wait until any and all updates made by the failed domain controller have been replicated to the domain controller seizing the role. This ensures that the changes that were made just prior to the failure of the original domain controller are not lost.
3. Ensure that the domain controller whose role was seized is never restored. It may have updates that it made but never replicated to the other domain controllers. The computer on which the role was seized must be removed from the domain.
4. Reformat the partition that contained the operating system files of the original operations master and reinstall Windows 2000 before reconnecting that computer to the network.

Lab A: Managing Operations Masters

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will learn how to determine the role of each operations master, transfer an operations master role from one domain controller to another, and seize an operations master role from a failed domain controller.



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

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Determine the operations master for each of the five roles.
- Transfer an operations master role to another domain controller.
- Seize an operations master role from a failed domain controller.
- Use Ntdsutil.exe to manage operations masters.

Prerequisites

Before working on this lab, you must have an understanding of the latency in Active Directory replication and how to initiate replication manually.

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.

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: 45 minutes

Exercise 1

Determining Operations Masters

Scenario

Northwind Traders is developing a disaster recovery plan. One important consideration is the distribution of the operations master roles. There will not be more than one operations master role on a domain controller. The operations master roles will be distributed across multiple domain controllers to minimize the impact of a failure at any one location.

Goal

In this exercise, you will determine which domain controller holds each of the two forest operations master roles, which are schema master and domain naming master. You will also determine which domain controller holds each of the three operations master roles in your domain, which are relative identifier (RID), primary domain controller (PDC) emulator, and infrastructure master. The three tasks will provide you with the necessary information for you to write your results in the following table. No role transfers or seizures are made in this exercise.

Operations Master	Domain Controller's FQDN
1. Schema	
2. Domain naming	
3. RID	
4. PDC emulator	
5. Infrastructure	

Tasks	Detailed Steps
1. Determine the current schema master by using the Active Directory Schema console.	- Log on as Administrator in your domain with a password of password. - In the Run box, type regsvr32.exe %systemroot%\system32\schmmgmt.dll and then click OK to register the Active Directory Schema snap-in. Click OK to close the message that indicates the registration succeeded. - In the Run box, type mmc click OK to open a new console, and then add the snap-in, Active Directory Schema. - In the console tree, expand Active Directory Schema. - In the console tree, right-click Active Directory Schema, and then click Operations Master. <i>If the role holder status displays 'ERROR', the connection was not attempted. You must click, or expand, the Active Directory Schema node (step d) before right-clicking it (step e).</i>

Tasks	Detailed Steps
 What additional step must you perform to transfer this role to your domain controller? You must first change the focus of the Active Directory Schema snap-in so that it will run on your computer, and then click Change in the Change Schema Master dialog box.	
1. (continued)	f. Using the information in the Change Schema Master dialog box, fill in line 1 of the table above with the name for the schema master. Note: The computer with the current focus, by default, is the schema master. g. Click Cancel to close the Change Schema Master dialog box, and then close the Active Directory Schema console without saving the settings.
2. Determine the current domain naming master by using the Active Directory Domains and Trusts console.	a. Open Active Directory Domains and Trusts from the Administrative Tools menu. b. Right-click Active Directory Domains and Trusts, and then click Operations Master. c. Using the information in the Change Operations Master dialog box, fill in line 2 of the table at the beginning of this lab with the FQDN for the domain naming master. d. Click Close to close the Change Operations Master dialog box, and then close Active Directory Domains and Trusts.
3. Determine the current role holder for the RID, PDC emulator, and infrastructure master by using the Active Directory Users and Computers console.	a. Open Active Directory Users and Computers from the Administrative Tools menu. b. In the console tree, right-click Active Directory Users and Computers, and then click Operations Masters. c. In the Operations Master dialog box, by using the information on each tab, fill in lines 3 through 5 of the table at the beginning of this lab with the FQDN for the RID, PDC emulator, and infrastructure master. d. Click Cancel to close the Operations Master dialog box, and leave Active Directory Users and Computers open.

Exercise 2

Transferring the Infrastructure Master Role

Scenario

After monitoring global catalog queries, Northwind Traders developed a plan to redistribute the global catalog server role among the domain controllers. Because the infrastructure master will not perform correctly on a global catalog, the plan also includes placement of this role on particular domain controllers.

Goal

In this exercise, you will transfer the infrastructure master role to the specified domain controller. It is recommended that the domain controller should be in the same site as a global catalog server, but it should not be on a global catalog server. This is because the infrastructure master frequently contacts a global catalog server.

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

Tasks	Detailed Steps
 Important: Perform the following task on both <i>infraser</i> (where <i>infraser</i> is the name of the infrastructure master) and <i>otherserver</i> (where <i>otherserver</i> is the name of the other domain controller in this domain).	
1. Verify the current holder of the infrastructure master role.	a. In Active Directory Users and Computers, in the console tree, right-click Active Directory Users and Computers , and then click Operations Masters . b. In the Operations Master dialog box, click the Infrastructure tab.  Notice that the current role holder is <i>infraser</i> .
 Important: Perform the following task on <i>otherserver</i> only.	
2. Transfer the infrastructure master role from <i>infraser</i> to <i>otherserver</i> .	a. In the Operations Master dialog box, click Change , and then click Yes to close the message confirming the transfer. b. Click OK to close the message indicating that the operations master role was successfully transferred, click OK again to close the Operations Master dialog, and then close Active Directory Users and Computers.
 Important: Perform the following task on <i>infraser</i> after the previous task is completed.	

Tasks	Detailed Steps
3. Verify that <i>infraserver</i> has been updated with the information that the transfer of the infrastructure master role took place.	a. To refresh the information displayed in the Operations Master dialog box, click Cancel to close the Operations Master dialog box in Active Directory Users and Computers. b. In the console tree, right-click Active Directory Users and Computers, and then click Operations Masters. c. In the Operations Master dialog box, click the Infrastructure tab. Notice that <i>otherserver</i> is now the infrastructure master role holder. d. Click Cancel to close the Operations Master dialog box, and then close Active Directory Users and Computers.

Exercise 3

Seizing the PDC Emulator Role

Scenario

The Northwind Traders Help Desk received an increasing number of complaints from users who run Windows NT version 4.0 on their computers stating that they are not able to change their passwords. The domain controller holding the PDC emulator role that performs this task has failed. The hardware part needed to repair the failed domain controller will take more than a week to acquire. Because this role performs critical operations, the Help Desk decided to seize the role from the domain controller. This was not a difficult decision because the domain was in native mode and there were no backup domain controllers (BDCs) that might have needed a full synchronization.

Goal

In this exercise, you will simulate a hardware failure on the domain controller by turning off the computer. Then you will seize the PDC emulator and give this role to another domain controller. You will then fix the simulated hardware failure and transfer the PDC emulator role back to the original domain controller.

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

Tasks	Detailed Steps
 Important: Perform the following task on <i>PDCserver</i> (where <i>PDCserver</i> is the name of the PDC emulator) only.	
1. Simulate a hardware failure by turning off <i>PDCserver</i> .	a. Close all open windows. b. Click Start , click Shut Down , click Shut down , and then click OK .
 Important: Perform the following task on <i>otherserver</i> (where <i>otherserver</i> is the name of the other domain controller in this domain) after the previous task is complete.	
2. Verify the current role holder of the PDC emulator by using Active Directory Users and Computers.	a. Open Active Directory Users and Computers from the Administrative Tools menu. b. In the console tree, right-click Active Directory Users and Computers, and then click Operations Masters.  <i>The Operations Masters dialog box may take a while to appear because it is waiting for a response from the RID master role holder. Expect a similar delay when clicking the other two operations master tabs.</i> c. In the Operations Master dialog box, click the PDC tab.

Tasks	Detailed Steps
 Is <i>otherserver</i> able to determine that the PDC emulator role holder is offline? Yes, <i>otherserver</i> attempted to contact this role holder and was unsuccessful. This attempt resulted in the text message stating ‘offline’ in the Operations Master dialog box.	
3. Seize the PDC emulator role from <i>PDCserver</i> and give it to <i>otherserver</i> by using Active Directory Users and Computers.	a. Although a message indicates that the role cannot be transferred, click Change, and then click Yes to close the confirmation message. b. Click OK to close the warning message that states “Transferring the PDC role to this machine may cause a full sync on all NT4 BDCs.” Note: This warning appears because the role transfer may cause a potentially large amount of network traffic when the BDCs are synchronized. This warning can be safely ignored because the domain is in native mode, meaning BDC synchronization cannot be performed.
 What was the operation that just failed? The cooperative transfer of the role failed because <i>PDCserver</i> could not be contacted.	
3. (continued)	c. Click OK to close the message indicating that a forced transfer was attempted.  The seize operation is being performed. d. Click OK to close the message indicating that the operations master role was successfully transferred. e. Click OK to close the Operations Master dialog box, and then close Active Directory Users and Computers.
 Important: Perform the following tasks on <i>PDCserver</i> after the previous task is complete.	
4. Start <i>PDCserver</i> and log on as Administrator.	▪ Start <i>PDCserver</i> and log on as Administrator.

Tasks	Detailed Steps
5. Initiate replication with <i>otherserver</i> by using Active Directory Sites and Services.	- Open Active Directory Sites and Services from the Administrative Tools menu. - Expand Sites, expand Default-First-Site-Name, and then expand Servers. - Expand <i>PDCserver</i>, and then click NTDS Settings. - Right-click a connection that is from <i>otherserver</i>, click Replicate Now, and then click OK to close the Replicate Now message indicating that replication occurred.  <i>If an error message appears stating that the RPC service is unavailable, wait a moment and try again. It may take some time for all of the necessary services to start after restarting the computer.</i> - Close Active Directory Sites and Services.
6. Verify that <i>PDCserver</i> has been updated with the information that the seizure of the PDC emulator role took place by using Active Directory Users and Computers.	- Open Active Directory Users and Computers from the Administrative Tools menu. - Right-click Active Directory Users and Computers, and then click Operations Masters. - In the Operations Master dialog box, click the PDC tab.
 How does <i>PDCserver</i> know that <i>otherserver</i> is now the PDC emulator? <i>PDCserver</i> knows that <i>otherserver</i> seized the role because the <i>otherserver's</i> data was replicated to <i>PDCserver</i>.	
7. Transfer the PDC emulator role from <i>otherserver</i> back to <i>PDCserver</i> .	- In the Operations Master dialog box, click Change to transfer the role holder back to the original server, <i>PDCserver</i>. - Click Yes to close the message confirming the transfer, click OK to close the message indicating the operations master role was successfully transferred, and then click OK to close the Operations Master dialog box. - Close Active Directory Users and Computers.

Exercise 4

Using ntdsutil to Transfer Operations Master Roles

Scenario

A consultant hired by Northwind Traders recommended a remote management strategy that used only command-line utilities. An additional goal was to perform these tasks from a telnet session.

Goal

In this exercise, you will use the command-line utility Ntdsutil.exe to determine all current role holders and to transfer the RID master.

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

Tasks	Detailed Steps
 Important: Perform the following tasks on both <i>RIDserver</i> (where <i>RIDserver</i> is the name of the RID master) and <i>otherserver</i> (where <i>otherserver</i> is the name of the other domain controller in this domain).	
1. Determine the current operations masters by using the ntdsutil utility.	- Open a command prompt window. - At the command prompt, type ntdsutil and then press ENTER. - At the ntdsutil prompt, type ? and then press ENTER to display the help information for this menu. Note: You can also view the help for any menu by typing ? or Help and then pressing ENTER. - At the ntdsutil prompt, type domain management and then press ENTER to display the domain management prompt. Note: You need to enter only enough letters of each keyword to distinguish it from each the others. For example, d m would be short for domain management. In addition, keywords are not case sensitive. - At the domain management prompt, type connections and then press ENTER to display the server connections prompt. - At the server connections prompt, type connect to server <i>servername</i> (where <i>servername</i> is the name of your computer), and then press ENTER. Note: If you want to connect to the server with different credentials from those of the locally logged on user, use set creds %s %s %s. View Help for more information. - At the server connections prompt, type info and then press ENTER to display the current connection information. - At the server connections prompt, type quit and then press ENTER to return to the domain management prompt. - At the domain management prompt, type select operation target and then press ENTER to display the select operation target prompt. - At the select operation target prompt, type list roles for connected server and then press ENTER to display all of the role holders this server knows about.

Tasks	Detailed Steps
1. <i>(continued)</i>	k. At the select operation target prompt, type quit and then press ENTER to return to the domain management prompt. l. At the domain management prompt, type quit and then press ENTER to return to the ntdsutil prompt.
2. View the maintenance options available in the ntdsutil utility.	a. At the ntdsutil prompt, type roles and then press ENTER to display the fsmo maintenance prompt. Note: fsmo (which stands for “flexible single master operation”) is the previous name for an operations master. b. At the fsmo maintenance prompt, type ? and then press ENTER to display all of the fsmo maintenance options. Notice that all seize and transfer operations are available.
 Important: Perform the following task on <i>otherserver</i> after the previous task is complete.	
3. Transfer the RID master role from <i>RIDserver</i> to <i>otherserver</i> by using ntdsutil .	a. At the fsmo maintenance prompt, type transfer RID master and then press ENTER. b. Click Yes to close the message confirming the transfer. Note: You can suppress these confirmation dialog boxes for use in automation or a telnet session. This is performed at the ntdsutil prompt by typing popups off. c. At the fsmo maintenance prompt, type quit and then press ENTER to return to the ntdsutil prompt.
 Important: Perform the following task on both <i>RIDserver</i> and <i>otherserver</i> after the previous task is complete.	
4. Close the ntdsutil utility and the command prompt window, and then log off.	a. At the ntdsutil prompt, type quit and then press ENTER to exit the utility. b. Close the command prompt window, close all other open windows, and then log off.

Best Practices

Topic Objective

To describe best practices for managing operations masters in Active Directory.

Lead-in

Let's discuss some best practices for managing operations masters in Active Directory.

- ✓ **Do Not Perform Frequent Role Transfers**
- ✓ **Transfer Operations Master Roles Before Demoting a Domain Controller**
- ✓ **Consider the Network Traffic for Password Changes When Assigning the PDC Emulator to a Domain Controller**
- ✓ **Review the Best Placement of Role Holders Periodically**
- ✓ **Assign the Schema and Domain Naming Master Roles to the Same Domain Controller**
- ✓ **Place a Global Catalog Server in the Same Site As the Infrastructure Master**

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

Describe the best practices for managing operations masters in Active Directory.

Consider the following best practices for using operations masters:

- Do not perform frequent role transfers. Perform role transfers only when making a major change to the domain infrastructure, such as when demoting a domain controller role holder, or when adding a new domain controller that is more suitable for some roles than the current holder.
- Transfer the operations master roles held by a domain controller before demoting the domain controller. This ensures that the transfer of a role is successful before you demote the domain controller. This also allows you to choose the new role holder and verify that the transfer is successful.
- Consider the network traffic associated with password changes when assigning the PDC emulator master role to a domain controller. Do this because there may be frequent network traffic from other domain controllers and pre-Windows 2000-based client computers because of user account password changes.
- Periodically review the best placement of the role holders in your network. The optimal placement of role holders may change because of network changes, usage patterns, or risk analysis.
- Assign the schema master and the domain naming master role to the same domain controller. It is easier to secure one domain controller than to secure two domain controllers, as would be necessary if the schema master and domain naming roles were on separate domain controllers. Also, the same group in an organization usually owns the domain controllers that hold the schema master and domain naming master roles.
- Place a global catalog server in the same site as the infrastructure master. This reduces network traffic when the infrastructure master enumerates its external references when updating them.

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 Operations Masters
- Operations Master Roles
- Managing Operations Master Roles
- Managing Operations Master Failures
- 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. Which operations masters are domain wide and which are forest wide?

The forest-wide operations masters are the schema master and the domain naming master. The domain-wide operations masters are the PDC emulator, the infrastructure master, and the RID master.

2. Which operations use the PDC emulator master role?

All PDC operations that support computers running pre-Windows 2000 versions of Windows, such as the synchronization with BDCs.

Minimizing latency issues with password changes.

Managing Time Synchronization.

Assuming the role of domain master browser.

3. Is there a way to get an operations master role back online when the current domain controller holding the role has been damaged beyond repair?

Yes. This is a seize operation. It is sometimes referred to as forceful transfer.

4. If the domain naming master were unavailable, which operations could not be performed?

Adding and removing domains from the forest could not be performed without the domain naming master. You also could not add new sites to the forest.

5. Why should you not seize the schema master role?

If a schema update had been recently made and had not yet been replicated to the domain controller that would receive the seized role, this update would be lost.

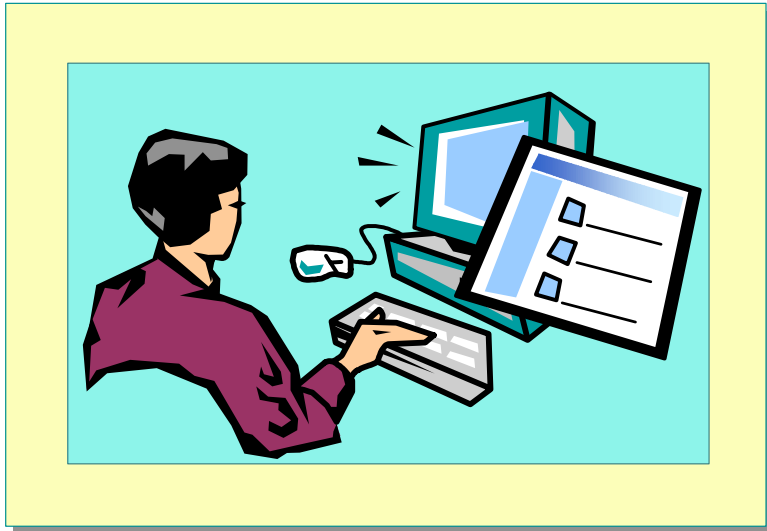
Course Evaluation

Topic Objective

To direct students to a Web site to complete a course evaluation.

Lead-in

Go to the Web site listed on this page to complete a course evaluation.



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

Your evaluation of this course will help Microsoft understand the quality of your learning experience.

At a convenient time between now and the end of the course, please complete a course evaluation, which is available at <http://www.metricsthatmatter.com/survey>.

Microsoft will keep your evaluation strictly confidential and will use your responses to improve your future learning experience.

