Windows 2000 Flexible Single-Master Operation

Architecture, deployment and management of FSMO roles

Written by	Paul Steunebrink, paul@steunebrink.nl
Date last revision	04 March 2002
Revision	1.3
Date created	04 March 2002
Date last saved	04 March 2002
Document previously named	WME_DROM.DOC

Table of Contents

1 Introduction....3
1.1 The single-master model....3
1.2 The multi-master model....3
1.3 The single-master operation....3
1.4 Other operation roles....3
2 FSMO Architecture....4
2.1 Explanation of FSMO roles....4
2.1.1 Forest wide FSMO roles....4
2.1.2 Domain wide FSMO roles....4
2.2 Implementation in AD design....4
3 FSMO Deployment....6
3.1 Deployment of FSMO roles....6
3.2 Implications for replication and management....6
4 FSMO Management....7
4.1 Recovering Operation Masters....7
4.1.1 Primary Domain Controller Emulator failures....7
4.1.2 Infrastructure Master failures....7
4.1.3 Other Operations Master Failures....7
4.1.4 Standy Operations Master domain controllers....8
4.1.5 FSMO administration....8
4.1.6 Default permission changing FSMO roles....8
5 Using the tools....9
5.1 Setting the domain mode....9
5.2 Identifying and transferring FSMO roles....9
5.2.1 Transfer the PDC Emulator, RID-, or Infrastructure Master....9
5.2.2 Transfer the Domain Naming Master....9
5.2.3 Transfer the Schema Master....10
5.3 Seizing FSMO roles....10
5.3.1 Seize the Relative ID Master....10
5.3.2 Seize the PDC Emulator....10
5.3.3 Seize the Infrastructure Master....11
5.3.4 Seize the Domain Naming Master....11
5.3.5 Seize the Schema Master....11
5.4 Setting up a Global Catalog server....12
5.5 Setting up a bridgehead server....12
6 FSMO.VBS script....13

1 Introduction

Windows 2000 domain controllers use a multi-master model in contrary to the single-master model of Windows NT from version 3.1 up to 4.0.

1.1 The single-master model

The single-master model describes one master, known as the Primary Domain Controller (PDC) and multiple 'slaves', known as Backup Domain Controller (BDC). The master holds a readable and write able copy of the directory database; the slave holds a readable copy only. The master through a process called replication periodically updates the slave.

1.2 The multi-master model

In Windows 2000 all domain controllers hold a readable and write able copy of the directory database. An algorithm known as the Knowledge Consistency Checker (KCC) figures out a replication topology. This process ensures a proper and effective replication between all domain controllers in the forest and domain.

1.3 The single-master operation

It appeared that in a multi-master model a number of operations should be hold by a single-master only, to prevent confusion. Applying a number of operations to a single domain controller only solves this problem. Only one (Windows 2000) domain controller holds the role for a particular operation and is therefore the single-master for that operation, like a PDC in a Windows NT environment. Note that a Windows 2000 domain controller can hold more single-master operation roles. The operations masters are also known as Flexible Single-Master Operation (FSMO) role. Flexible relates to the ability to transfer a role to a different domain controller.
This document explains the different single-master operation roles, how the can be identifi ed and transferred and their recovery in case of a disaster.

1.4 Other operation roles

Windows 2000 domain controllers can also act as Global Catalog server and as a preferred bridgehead server for a site. Note that these roles are NOT single-master, that is, more than one domain controller within the domain or forest can hold such a role. On the other hand, a

2 FSMO Architecture

2.1 Explanation of FSMO roles

FSMO stands for Flexible Single-Master Operation. A Windows 2000 domain controller can hold one or more FSMO roles. A FSMO role is a specific kind of functionality related to the Windows 2000 Active Directory Service, which is unique within the forest or the domain. Two forest wide FSMO roles exist and three domain wide FSMO roles. The total number of FSMO roles in a forest, depends on the number of domains in that forest. In a forest with two domains, there are eight (2+(2*3)) FSMO roles. The FSMO roles and there functionality are explained below.

2.1.1 Forest wide FSMO roles

Two forest wide FSMO roles exist: the Schema Master and the Domain Naming Master.

- Schema Master can perform write operations to the directory schema. Those schema updates are replicated from the Schema Master to all other domain controllers in the forest.
- Domain Naming Master can add or remove domains in the forest and add or remove cross-reference objects to external directories.

2.1.2 Domain wide FSMO roles

Three domain wide FSMO roles exist: the Relative ID Master, the PDC Emulator and the Infrastructure Master.

- Relative ID (RID) Master manages the relative identifiers for all the domain controllers in the domain by periodically creating and RID pool for a domain controller. This enables that domain controller to create several hundreds of security principal objects (User, Group, or Computer) with a unique number within the Active Directory.
- PDC Emulator serves as a Primary Domain Controller for Windows NT 4.0 and 3.51 systems if the are available as Backup Domain Controller in the domain. Note that this task is related to the Mixed mode domain mode. When a domain has changed its domain mode to Native, this task no longer exists.
  The PDC Emulator also handles discrepancies between an old and renewed password, which not yet had fully been replicated.
  Time synchronisation in a forest and in the domain, required for the Kerberos authentication protocol, is also handled by the PDC Emulator. All systems refer to the PDC Emulator of their domain to synchronise the time. All PDC Emulator synchronise with the PDC Emulator of the forest root domain – first domain in the forest – and is therefore authoritative for the enterprise in this respect. This explains why (only) the domain controller of the forest root domain that holds PDC Emulator role must be connected to an external time source.
  In addition, Windows NT domains use the PDC location information to establish trusts.
  Finally, the PDC Emulator is also the reference point for creating and updating Group Policies. This setting is default but can be overruled.
- Infrastructure Master is responsible for updating the cross-domain group-to-user reference to reflect for example a user's new name after renaming the name. The Infrastructure Master updates these references locally and uses replication to bring all other replicas of the domain up to date.

2.2 Implementation in AD design

The main design goal, regarding the FSMO roles, is performance. The best possible placement of the FSMO roles depends on use, the Active Directory structure (logically, physically), available bandwidth and replication needs, and system management.
Besides the FSMO roles, a domain controller can be a Global Catalog server and a (preferred) bridgehead server for replication. For optimal performance, there are three general recommendations for FSMO placement and the Global Catalog (according to Microsoft Knowledgebase article Q223346). A fourth recommendation is added for maintenance.

1. Place the RID Master and PDC Emulator roles on the same domain controller. If the load on the FSMO justifies a move, place the RID and PDC emulator roles on separate domain controllers that have direct connection objects to the standby RID Master and PDC Emulator.
2. A non-Global Catalog server that has a direct connection object to some Global Catalog servers in the forest, preferably in the same Active Directory site should hold the Infrastructure Master. If this role is hosted on a GC server, cross-domain object references in that domain are not updated, and an error to that effect is entered in that DC's event log (ID: 1419, source: NTDS General). Therefore, do not place

the Infrastructure Master on a GC!
Note: a forest that consists of a single domain controller is the only exception to this rule.

3. At the forest level, the Schema Master and Domain Naming Master roles should be placed on the same domain controller as they are rarely used and should be tightly controlled. Additionally, the Domain Naming Master FSMO should also be a Global Catalog server.
4. Save an additional domain controller per domain WITHOUT any FSMO role. This provides space and flexibility for transferring FMSO roles to from a server that needs maintenance or has crashed. This domain controller is called the (FSMO) standby server.

3 FSMO Deployment

3.1 Deployment of FSMO roles

During deployment of the domains and the domain controllers within these domains, the FSMO roles are created and placed automatically. The first domain controller in the forest receives all the five FSMO roles (forest and domain wide roles) and will be the Global Catalog server as well. The second and next domain controllers in the same domain will only hold a FSMO role if it is transferred manually by hand or script. The first domain controller in a new created domain in the same forest, weather or not in the same tree, will hold all three domain wide FSMO roles. Additional domain controllers within that domain will hold a FSMO role if it is transferred manually by hand or script.
This placement works well for a forest deployed on a few domain controllers in a single site. In a forest with more domain controllers or multiple sites, you need to plan the placement of operations master roles carefully to match your replication and network topologies.
Considering the general recommendations for placement of FSMO roles, the operations masters are implemented according the table below. In this example the forest exists of two domains, called root and branch. In a central site each domain has three domain controllers. The branch domain has numerous domain controllers in their respective branch offices.
Note that the Global Catalog (GC) and bridgehead server are mentioned also, as well as DNS.

Servers	Domain	SM	DNM	RID	PDC	IM	GC	BH	DNS
	(NetBIOS)	(forest wide)		(domain wide)					
DCFR001	root	X	X				X		X
DCFR002	root			X	X	X			X
DCFR003	root								
DCBR001	branch			X	X	X			X
DCBR002	branch						X	X	X
DCBR003	branch						X	X	
all DC's in branch offices	branch								

Legend:

SM	Schema Master
DNM	Domain Naming Master
RID	Relative ID Master
PDC	PDC emulator
IM	Infrastructure Master
GC	Global Catalog server
BH	Preferred bridgehead server
DNS	Domain Name System server

3.2 Implications for replication and management

Managing the FSMO roles is discussed in detail in the next paragraph. The following statements can be a guideline in management.

- The domain controller(s) in the forest root domain hold forest and domain wide FSMO roles respectively. It is suggested these domain controller(s) act as each other's backup if there are two of them. Put in other words, if one should fail, the other should or could take over its FSMO roles. Three domain controllers in the forest root are highly preferable to create one FSMO-standby domain controller.
- In the branch domain, the DCBR001 is the only owner of FSMO roles. The DCBR002 or DCBR003 can be configured to hold the FSMO roles in case the DCBR001 should fail. They both are configured as Global Catalog and preferred bridgehead server, to perform intersite replication. In case of transfer of the IM role to the DCBR002 or –3, this server should become a non-Global Catalag (temporarily).

4 FSMO Management

In general, FSMO roles do not need any management. Once set, they stay in place. However, in case of a system failure or changes to the domain or forest configuration or changes to domain replication, management may be necessary.
This section describes how to act when a system failure makes a FSMO role unavailable. Some questions to answer are:

- What functionality is lost when a domain controller holding an operations master role is unavailable?
- When a domain controller holding an operations master role is unavailable for an extended period, how do you respond to restore the service?
- How to recover a disruption of the availability of a FSMO role?

4.1 Recovering Operation Masters

4.1.1 Primary Domain Controller Emulator failures

The loss of a domain controller that is the PDC Emu lator role will not immediate be visible to the user or administrator if only Windows 2000 systems are used. If Windows NT or Windows 9x systems are used and no Windows NT BDC exists, you are in real trouble because the NT/9x systems can no longer logon.
The PDC Emulator plays a main role in time synchronisation between DC's and the workstations, and when creating or changing a GPO (Group Policy Object), the PDC Emulator is the main focus between all other DC's.
If external trusts exist with Windows NT domains, these trust can be broken if the PDC Emulator fails.
If the PDC Emulator is offline for a significant period of time, you should seize the PDC Emulator role to another domain controller.
The user interface for this seizure is similar to that of a normal operations master role transfer, except it requires an extra confirmation from you. Agree to the confirmation *only* if you know the current PDC Emulator will be offline for a significant period. Later, when the original PDC Emulator domain controller comes back online, transfer the role back to the original role owner.

4.1.2 Infrastructure Master failures

Temporary loss of a domain's infrastructure master is not visible to end users, and is not visible to you, as an administrator, unless you recently moved or renamed a large number of accounts. Therefore, in most cases, a temporary loss of the infrastructure master is not a problem worth fixing.
If you anticipate a long outage of a domain's infrastructure master and you need to repair it, first select a domain controller that is not a Global Catalog server and that has good network connectivity to a Global Catalog server located in any domain. Ideally, the domain controller you have chosen should be within the same site as a Global Catalog server. It is not important that the new infrastructure master be near the previous one. When you have selected the domain controller, seize the infrastructure master role to this domain controller.
The user interface for this seizure is similar to that of a normal operations master role transfer, except it requires an extra confirmation from you. Agree to the confirmation *only* if you know that the current infrastructure master will be offline for a very long period. Later, when the original infrastructure master comes back online, transfer the role back to the original role owner.

4.1.3 Other Operations Master Failures

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 *drastic* step; one 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.
A domain controller, whose Schema Master, Domain Naming Master, or RID master role is seized, must *never* come back online with its contents of Active Directory. Format its disk before reinstalling.
Before proceeding with the role seizure, you must ensure that the outage of this domain controller is permanent by physically disconnecting the domain controller from the network.
The domain controller that seizes the role should be fully up-to-date with respect to updates performed on the previous role owner. Because of replication latency, it is possible that the domain controller might not

be up-to-date.
For further details, please see the Windows 2000 Server Resource Kit, Chapter 7 Managing Flexible Single-Master Operations.

> (…)
> *Weather or not to use a backup to restore a DC with FSMO role depends on the choice of seizing a FSMO role. If the role is seized, do not use the backup to restore the system. If the role was not seized, reinstall the system, promote it to a DC en perform a non-authoritative restore.*

4.1.4 Standy Operations Master domain controllers

In the previous section, the term 'Standby Operations Master domain controllers' was used. This is not a DC with one kind of special setup. It is one of the DC's, which is you first choice if you need to transfer or seize a FSMO role to in case that role is not available on the network due to a failure of the DC that holds that role.

4.1.5 FSMO administration

FSMO roles can be viewed, transferred and seized.

1. Viewing FSMO roles
   FSMO roles can be viewed with de MMC tool, as well as by running a VBS script.
2. Transferring FSMO roles
   If a DC, that holds one or more FSMO roles, needs to be taken offline, the FSMO role(s) needs to be transferred in advance. When the system becomes online again, the FSMO role(s) should be transferred back again. The same counts for demoting a domain controller with a FSMO role.
3. Seizing FSMO roles
   If a DC, that holds one or more FSMO roles, goes accidentally offline (i.e. a crash), the FSMO role(s) could not be transferred in advance. Therefore, it has to be seized as quickly as possible after the accident occurred. After the system is repaired, the role has to be transferred back again.
   Warning: A DC whose FSMO roles include Schema Master, Domain Naming Master or RID Master should never be brought online again without first reformatting the drives and reloading Windows 2000 Server.

A number of tools can be used to administrate FSMO roles: MMC snap-in admintools, VBS-script or NTDSUTIL.EXE.

- Viewing FSMO roles: ..... MMC, FSMO.VBS
- Transferring FSMO roles:..... MMC, NTDSUTIL.EXE
- Seizing FSMO roles: ..... NTDSUTIL.EXE

For a details description of the tools, see section *5 Using the tools* and *6 FSMO.VBS script*.

4.1.6 Default permission changing FSMO roles

The table below outlines de default permissions that are required to change a FSMO role

FSMO role	Default Permission
Schema Master	Schema Administrators
Domain Naming Master	Enterprise Administrators
RID Master	Domain Administrators
PDC Emulator	Domain Administrators
Infrastructure Master	Domain Administrators

5 Using the tools

This chapter brings all the necessary tools and the way to use them together to manage your FSMO roles, Global Catalog and bridgehead server. The experienced system administrator can easily skip the previous chapters and use this chapter as a reference.
Maintaining a network infrastructure is an art of continuous learning.

5.1 Setting the domain mode

- Task:
  Change the domain mode of an ADS domain from Mixed mode to Native mode.
- Tool:
  Active Directory Domains and Trusts
- Action:
  Select the proper domain. Open the properties of that domain. On the General tab of the domain properties sheet, view the Domain operation mode. If the domain is in Mixed mode, click on the Change Mode button. Click OK to close the properties sheet.

5.2 Identifying and transferring FSMO roles

Transferring these roles is part op proactive maintenance. For seizing these roles, see the paragraph below. Because identifying an FSMO role is the first step in transferring a role, both identifying and transferring are described in this paragraph.

5.2.1 Transfer the PDC Emulator, RID-, or Infrastructure Master

Note: In order to be able to transfer each one of these roles, the user must be a member of the Domain Admins group for that domain.

- Task:
  Identify or transfer the PDC Emulator, Relative ID Master, or Infrastructure Master (domain wide FSMO role) operations master to another domain controller.
- Tool:
  Active Directory Users and Computers
- Action:
  Open Active Directory Users and Computers.
  Identifying: Connect to any domain controller in the domain for which the PDC Emulator, Relative ID Master, or Infrastructure Master operations master needs to be identified. Right-click **Active Directory Users and Computers** and click **Operations Masters**. View the operations masters on each of the three tabs RID, PDC and Infrastructure.
  Transferring: Connect to the domain controller that will become the new holder of the FSMO role. Right-click **Active Directory Users and Computers** and click **Operations Masters**. Click on the **Change** button for each of the operations master you want to transfer.

5.2.2 Transfer the Domain Naming Master

Note: In order to be able to transfer this role, the user must be a member of the Enterprise Admins group.

- Task:
  Identify or transfer the Domain Naming Master (forest wide) operations master role to another domain controller.
- Tool:
  Active Directory Domains and Trusts
- Action:
  Open Active Directory Domains and Trusts.
  Identifying: Connect to any domain controller in the forest. Right-click **Active Directory Domains and Trusts** and click **Operations Masters**. The name of the current Domain Naming master appears in **Domain Naming operations master**.
  Transferring: Connect to the domain controller that will become the new holder of the Domain Naming Master role.
  Open the *Change Operations Master* dialog box by choosing **Operations Master** in the **Action** menu.

Tip: Do not select the domain, but select the root of the tree in the left pane.

View the name of the current holder of the Domain Naming operations masters. Click on the Change button to transfer the role to the domain controller you are connected to.

5.2.3 Transfer the Schema Master

Note: In order to be able to transfer this role, the user must be a member of the Schema Admins group.

- Task:
  Identify or transfer the Schema Master (forest wide) operations master role to another domain controller.
- Tool:
  Active Directory Schema
  Note: first register the Schema-DLL, before you can add the Active Directory Schema to a MMC with the command.
  (`regsvr32.exe schmmgmt.dll`)
- Action:
  Open Active Directory Schema.
  Identify : In the console tree, right-click **Active Directory Schema** and then click **Operations Master**. The name of the current domain naming master appears in **Current Operations Master**.
  Transfer: In the console tree, right-click **Active Directory Schema** and then click **Change Domain Controller**. Click **Specify Name** and type the name of the new schema master computer. In the console tree, right-click **Active Directory Schema**, and then click **Operations Master**. Click **Change**.

5.3 Seizing FSMO roles

Seizing these roles is part op reactive maintenance. To identify or transfer each of these roles, see the paragraph above.
Seize a role if the domain controller is accidentally not on-line and a transfer is not available as an option. If a role is seized, never bring the DC on-line again. Always reinstall the server from scratch. Do not use a restore of a backup that was made when the DC did hold the seized role.

5.3.1 Seize the Relative ID Master

- Task:
  Seize the Relative ID Master role to a specified domain controller
- Tool:
  NTDSUTIL.EXE (command line tool)
- Action:
  1. Open a Command Prompt. Start Ntdsutil.
  2. At the **ntdsutil** prompt, type **roles**.
  3. At the **fsmo maintenance** prompt, type **connections**.
  4. At the **server connections** prompt, type **connect to server**, followed by the fully qualified domain name.
  5. At the **server connections** prompt, type **quit**.
  6. At the **fsmo maintenance** prompt, type **seize RID master**.
  7. At the **fsmo maintenance** prompt, type **quit**.
  8. At the **ntdsutil** prompt, type **quit**.

  Caution: Seizing the relative ID master is a drastic step that should be considered only if the current operations master will never be available again.
  Note: Before seizing the relative ID master, use Repadmin, in the Active Directory support tools, to verify whether the new operations master has received any updates performed by the previous role holder, and then remove the current operations master from the network.

5.3.2 Seize the PDC Emulator

- Task:
  Seize the PDC Emulator role to a specified domain controller
- Tool:
  NTDSUTIL.EXE (command line tool)
- Action:
  1. Open a Command Prompt. Start Ntdsutil.
  2. At the **ntdsutil** prompt, type **roles**.

3. At the **fsmo maintenance** prompt, type **connections**.
4. At the **server connections** prompt, type **connect to server**, followed by the fully qualified domain name.
5. At the **server connections** prompt, type **quit**.
6. At the **fsmo maintenance** prompt, type **seize PDC**.
7. At the **fsmo maintenance** prompt, type **quit**.
8. At the **ntdsutil** prompt, type **quit**.

Notes: Before seizing the PDC emulator master, remove the current operations master from the network and verify that the new operations master is up to date.
When the original PDC emulator master has returned to service, you can return the role to the original domain controller.

5.3.3 Seize the Infrastructure Master

- Task:
  Seize the Infrastructure Master role to a specified domain controller
- Tool:
  NTDSUTIL.EXE (command line tool)
- Action:
  1. Open a Command Prompt. Start Ntdsutil.
  2. At the **ntdsutil** prompt, type **roles**.
  3. At the **fsmo maintenance** prompt, type **connections**.
  4. At the **server connections** prompt, type **connect to server**, followed by the fully qualified domain name.
  5. At the **server connections** prompt, type **quit**.
  6. At the **fsmo maintenance** prompt, type **seize infrastructure master**.
  7. At the **fsmo maintenance** prompt, type **quit**.
  8. At the **ntdsutil** prompt, type **quit**.

  Notes: Before seizing the infrastructure master, remove the current operations master from the network and verify that the new operations master is up to date.
  When the original infrastructure master has returned to service, you can transfer the role back to the original domain controller.

5.3.4 Seize the Domain Naming Master

- Task:
  Seize the Domain Naming Master role to a specified domain controller
- Tool:
  NTDSUTIL.EXE (command line tool)
- Action:
  1. Open a Command Prompt. Start Ntdsutil.
  2. At the **ntdsutil** prompt, type **roles**.
  3. At the **fsmo maintenance** prompt, type **connections**.
  4. At the **server connections** prompt, type **connect to server**, followed by the fully qualified domain name.
  5. At the **server connections** prompt, type **quit**.
  6. At the **fsmo maintenance** prompt, type **seize domain naming master**.
  7. At the **fsmo maintenance** prompt, type **quit**.
  8. At the **ntdsutil** prompt, type **quit**.

  Caution: Seizing the Domain Naming Master is a drastic step that should be considered only if the current operations master will never be available again.
  Note: Before seizing the Domain Naming Master, remove the current operations master from the network and verify that the new operations master is up to date.

5.3.5 Seize the Schema Master

- Task:
  Seize the Schema Master role to a specified domain controller
- Tool:
  NTDSUTIL.EXE (command line tool)
- Action:
  1. Open a Command Prompt. Start Ntdsutil.

2. At the **ntdsutil** prompt, type **roles**.
3. At the **fsmo maintenance** prompt, type **connections**.
4. At the **server connections** prompt, type **connect to server**, followed by the fully qualified domain name.
5. At the **server connections** prompt, type **quit**.
6. At the **fsmo maintenance** prompt, type **seize schema master**.
7. At the **fsmo maintenance** prompt, type **quit**.
8. At the **ntdsutil** prompt, type **quit**.

Caution: Seizing the Schema Master is a drastic step that should be considered only if the current operations master will never being available again.
Note: Before seizing the Schema Master, remove the current operations master from the network and verify that the copy of the schema on the new operations master is up to date with the rest of the domain controllers in the forest.

5.4 Setting up a Global Catalog server

- Task:
  Select or deselect a domain controller as Global Catalog server
- Tool:
  Active Directory Sites and Services
- Action:
  Select the server in the left pane (Tree) under Sites, <site name> (typically CCA), Servers. Select the NTDS Settings of that server in the left pane. Open the properties. On the General tab of the properties sheet, view the Global Catalog option (checked or not). Change according to plan. Click OK.

Tip: If there is only one GC in a domain, that you like to move, first set at least one different GC on another server and wait twenty minutes for intra-site replication to occur.

Note: The Infrastructure Master should be held by a non-Global Catalog server that has a direct connection object to some Global Catalog in the forest, preferably in the same Active Directory site. If the Infrastructure Master role is hosted on a GC server, cross-domain object references in that domain are not updated, and an error to that effect is entered in that DC's event log (ID: 1419, source: NTDS General). If there is a single domain controller for a domain, the error will not occur in the log.

5.5 Setting up a bridgehead server

- Task:
  Enable or disable a domain controller for inter-site data transfer (replication) for a specific transport, a.k.a. bridgehead server.
- Tool:
  Active Directory Sites and Services
- Action:
  Select the server in the left pane (Tree) under Sites, <site name> (typically CCA), Servers. Open the properties. On the Server tab of the properties sheet, view the available transports for inter-site data transfer. Add or remove a transport (default IP, not SMTP) according to plan. Click OK.

6 FSMO.VBS script

This Visual Basic Script can be used to read the different FSMO roles in the forest. This script is derived from Microsoft TechNet article Q235617.

```
   Option Explicit
  Dim WSHNetwork, objArgs, ADOconnObj, bstrADOQueryString, RootDom, RSObj
  Dim FSMOobj,CompNTDS, Computer, Path, HelpText

   Set WSHNetwork = CreateObject("WScript.Network")
  Set objArgs = WScript.Arguments

   HelpText = "This script will find the FSMO role owners for your domain." & Chr(13) &_
              Chr(10) & "The syntax is as follows:" & Chr(13) & Chr(10) &_
              "find_fsmo DC=MYDOM,DC=COM" & Chr(13) & Chr(10) &_
             """Where MYDOM.COM is your domain name."""" & Chr(13) & Chr(10) & "OR:" &_
              Chr(13) & Chr(10) & "find_fsmo MYDCNAME " & Chr(13) & Chr(10) &_
              """Where MYDCNAME is the name of a Windows 2000 Domain Controller"""

   Select Case objArgs.Count
      Case 0
          Path = InputBox("Enter your DC name or the DN for your domain"&_
                          " 'DC=MYDOM,DC=COM':","Enter path",WSHNetwork.ComputerName)
      Case 1
          Select Case UCase(objArgs(0))
              Case "?"
                  WScript.Echo HelpText
                  WScript.Quit
              Case "/?"
                  WScript.Echo HelpText
                  WScript.Quit
              Case "HELP"
                  WScript.Echo HelpText
                  WScript.Quit
              Case Else
                  Path = objArgs(0)
          End Select
      Case Else
          WScript.Echo HelpText
          WScript.Quit
  End Select

   Set ADOconnObj = CreateObject("ADODB.Connection")

   ADOconnObj.Provider = "ADSDSOObject"
  ADOconnObj.Open "ADs Provider"

   'PDC FSMO
  bstrADOQueryString =
"<LDAP://"&Path&">;(&(objectClass=domainDNS)(fSMORoleOwner=*));adspath;subtree"
  Set RootDom = GetObject("LDAP://RootDSE")
  Set RSObj = ADOconnObj.Execute(bstrADOQueryString)
  Set FSMOobj = GetObject(RSObj.Fields(0).Value)
  Set CompNTDS = GetObject("LDAP://" & FSMOobj.fSMORoleOwner)
  Set Computer = GetObject(CompNTDS.Parent)
  WScript.Echo "The PDC FSMO is: " & Computer.dnsHostName

   'Rid FSMO
  bstrADOQueryString =
"<LDAP://"&Path&">;(&(objectClass=rIDManager)(fSMORoleOwner=*));adspath;subtree"

   Set RSObj = ADOconnObj.Execute(bstrADOQueryString)
  Set FSMOobj = GetObject(RSObj.Fields(0).Value)
  Set CompNTDS = GetObject("LDAP://" & FSMOobj.fSMORoleOwner)
  Set Computer = GetObject(CompNTDS.Parent)
  WScript.Echo "The RID FSMO is: " & Computer.dnsHostName

   'Infrastructure FSMO
  bstrADOQueryString =
"<LDAP://"&Path&">;(&(objectClass=infrastructureUpdate)(fSMORoleOwner=*));adspath;subtree
"

   Set RSObj = ADOconnObj.Execute(bstrADOQueryString)
  Set FSMOobj = GetObject(RSObj.Fields(0).Value)
  Set CompNTDS = GetObject("LDAP://" & FSMOobj.fSMORoleOwner)
```

```
  Set Computer = GetObject(CompNTDS.Parent)
  WScript.Echo "The Infrastructure FSMO is: " & Computer.dnsHostName

   'Schema FSMO
  bstrADOQueryString = "<LDAP://"&RootDom.Get("schemaNamingContext")&_
                       ">;(&(objectClass=dMD)(fSMORoleOwner=*));adspath;subtree"

   Set RSObj = ADOconnObj.Execute(bstrADOQueryString)
  Set FSMOobj = GetObject(RSObj.Fields(0).Value)
  Set CompNTDS = GetObject("LDAP://" & FSMOobj.fSMORoleOwner)
  Set Computer = GetObject(CompNTDS.Parent)
  WScript.Echo "The Schema FSMO is: " & Computer.dnsHostName

   'Domain Naming FSMO
  bstrADOQueryString = "<LDAP://"&RootDom.Get("configurationNamingContext")&_

">;(&(objectClass=crossRefContainer)(fSMORoleOwner=*));adspath;subtree"

   Set RSObj = ADOconnObj.Execute(bstrADOQueryString)
  Set FSMOobj = GetObject(RSObj.Fields(0).Value)
  Set CompNTDS = GetObject("LDAP://" & FSMOobj.fSMORoleOwner)
  Set Computer = GetObject(CompNTDS.Parent)
  WScript.Echo "The Domain Naming FSMO is: " & Computer.dnsHostName
```