

# Re: Multihomed Domain Controller Setup

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2005-12/msg00653](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2005-12/msg00653)

---

- *From:* "Ace Fekay [MVP]" <PleaseSubstituteMyActualFirstName&LastNameHere@xxxxxxxxxxxx>
  - *Date:* Sat, 10 Dec 2005 12:59:50 -0500
- 

In [news:BDA871AA-DAD4-4CCA-B30F-57F9E8A1C6FE@xxxxxxxxxxxx](mailto:news:BDA871AA-DAD4-4CCA-B30F-57F9E8A1C6FE@xxxxxxxxxxxx), bishop <bishop@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> stated, which I commented on below:

- > Hi,
- >
- > I recently upgraded my domain from Windows 2000 Active Directory to
- > Windows 2003 AD. I added new servers that have two NICs in them and
- > am getting the usual browser problem. Everywhere I read said that DCs
- > should not be multihomed but, I have multiple live public subnets and
- > one internal subnet so that the DCs can have network access to the
- > internal subnet computers.
- >
- > Should I not use the second NICs and connect all DCs to live subnets
- > only? if so, will the internal subnet clients authenticate okay and
- > get the GPOs applied correctly?
- > Does the clients pull GPOs or servers push? if the clients pull, then
- > there really is no reason for the DCs to be on the internal subnet
- > since they won't need network access to them other than for GPOs, is
- > this right?

IN addition to Mark's suggestions (good link he provided!), if you want to keep the extra NIC turned on (for whatever reason, but I really suggest to disable it), here are some extra steps to follow:

1. Insure that all the NICS only point to your internal DNS server(s) only and none others, such as your ISP's DNS servers' IP addresses.
2. In Network & Dialup properties, Advanced Menu item, Advanced Settings, move the internal NIC (the network that AD is on) to the top of the binding order (top of the list).
3. Disable the ability for the outer NIC to register. The procedure, as mentioned, involves identifying the outer NIC's GUID number. This link will show you how:  
246804 – How to Enable–Disable Windows 2000 Dynamic DNS Registrations (per NIC too):  
<http://support.microsoft.com/?id=246804>

## Re: Multihomed Domain Controller Setup

4. Disable NetBIOS on the outside NIC. That is performed by choosing to disable NetBIOS in IP Properties, Advanced, and you will find that under the "WINS" tab. You may want to look at step #3 in the article to show you how to disable NetBIOS on the RRAS interfaces if this is a RRAS server.

296379 – How to Disable NetBIOS on an Incoming Remote Access Interface [Registry Entry]:

<http://support.microsoft.com/?id=296379>

Note: A standard Windows service, called the "Browser service", provides the list of machines, workgroup and domain names that you see in "My Network Places" (or the legacy term "Network Neighborhood"). The Browser service relies on the NetBIOS service. One major requirement of NetBIOS service is a machine can only have one name to one IP address. It's sort of a fingerprint. You can't have two brothers named Darrell. A multihomed machine will cause duplicate name errors on itself because Windows sees itself with the same name in the Browse List (My Network Places), but with different IPs. You can only have one, hence the error generated.

5. Disable the "File and Print Service" and disable the "MS Client Service" on the outer NIC. That is done in NIC properties by unchecking the respective service under the general properties page. If you need these services on the outside NIC (which is unlikely), which allow other machines to connect to your machine for accessing resource on your machine (shared folders, printers, etc.), then you will probably need to keep them enabled.

6. Uncheck "Register this connection" under IP properties, Advanced settings, "DNS" tab.

7. Delete the outer NIC IP address, disable Netlogon registration, and manually create the required records

a. In DNS under the zone name, (your DNS domain name), delete the outer NIC's IP references for the "LdapIpAddress". If this is a GC, you will need to delete the GC IP record as well (the "GcIpAddress"). To do that, in the DNS console, under the zone name, you will see the \_msdcs folder. Under that, you will see the \_gc folder. To the right, you will see the IP address referencing the GC address. That is called the GcIpAddress. Delete the IP addresses referencing the outer NIC.

i. To stop these two records from registering that information, use the steps provided in the links below:

Private Network Interfaces on a Domain Controller Are Registered in DNS <http://support.microsoft.com/?id=295328>

ii. The one section of the article that disables these records is done with this registry entry:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters  
(Create this Multi-String Value under it):

Registry value: DnsAvoidRegisterRecords

Data type: REG\_MULTI\_SZ

Re: Multihomed Domain Controller Setup

Values: LdapIpAddress  
GcIpAddress

iii. Here is more information on these and other Netlogon Service records:  
Restrict the DNS SRV resource records updated by the Netlogon service  
[including GC]:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standa>

b. Then you will need to manually create these two records in DNS with the IP addresses that you need for the DC. To create the LdapIpAddress, create a new host under the domain, but leave the "hostname" field blank, and provide the internal IP of the DC, which results in a record that looks like:  
(same as parent) A 192.168.5.200 (192.168.5.200 is used for illustrative purposes)

i. You need to also manually create the GcIpAddress as well, if this is a GC. That would be under the gc.\_msdcs. SRV record under the zone. It is created in the same fashion as the LdapIpAddress mentioned above.

8. In the DNS console, right click the server name, choose properties, then under the "Interfaces" tab, force it only to listen to the internal NIC's IP address, and not the IP address of the outer NIC.

9. Since this is also a DNS server, the IPs from all NICs will register, even if you tell it not to in the NIC properties. See this to show you how to stop that behavior (this procedure is for Windows 2000, but will also work for Windows 2003):  
275554 – The Host's A Record Is Registered in DNS After You Choose Not to Register the Connection's Address:  
<http://support.microsoft.com/?id=275554>

--  
Ace

This posting is provided "AS-IS" with no warranties or guarantees and confers no rights.

Ace Fekay, MCSE 2003 & 2000, MCSA 2003 & 2000, MCSE+I, MCT, MVP  
Microsoft MVP – Windows Server Directory Services  
Microsoft Certified Trainer  
Assimilation Imminent. Resistance is Futile.  
Infinite Diversities in Infinite Combinations.

=====

.

---

• *Follow-Ups:*

Re: Multihomed Domain Controller Setup

◆ **Re: Multihomed Domain Controller Setup**

◇ From: bishop

- Prev by Date: **Re: Can't browse shares in trusted domain from Client**
- Next by Date: **Re: Active Directory Replication error**
- Previous by thread: **Re: Multihomed Domain Controller Setup**
- Next by thread: **Re: Multihomed Domain Controller Setup**
- Index(es):
  - ◆ **Date**
  - ◆ **Thread**