

# Re: AD DC registering private IP as AD DNS

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2005-04/msg00812.html>

---

- *From:* "Ace Fekay [MVP]" <PleaseSubstituteMyActualFirstName&LastNameHere@xxxxxxxxxxxx>
  - *Date:* Thu, 28 Apr 2005 00:48:41 -0400
- 

ErMaC wrote:

- > Okay, so we have a Server 2003 Domain Controller which also runs DNS.
- > It has two network connections– one on a private crossover connection
- > to another machine (for fast file transfer backups that don't clog
- > the network) and the main one that has a public IP, etc.
- >
- > At first, both the machine name (server.domain.blah) and the domain
- > name itself (domain.blah) were being given A Host records with the
- > private IP. Unchecking the "register this connection's IP in DNS" box
- > on the private interface didn't help. I found a knowledge base
- > article that said to remove the adapter/IP address from the
- > "listening" options on the DNS server, and that seems to have fixed
- > half the problem.
- >
- > Now, server.domain.blah no longer registers 192.168.1.2, but
- > domain.blah still contains the private address along with the IP
- > addresses of the other domain controllers. I've tried both the other
- > potential fixes listed in various KB articles – adding a
- > "PublishAddresses" reg key to the DNS registry key, and adding a
- > "DisableDynamicUpdate" value to the interface and setting it to 1.
- > I've also tried changing the DNS Suffix of the connection to NOT be
- > domain.blah, but it STILL registers, and it's driving me NUTS.
- >
- > Does anyone know why it's registering in the domain.blah but not
- > server.domain.blah? How can I fix this?

You are seeing the LdapIpAddress being registered, which is what ALL DCs register to identify themselves as a DC in the domain.

To stop that, you'll need to disable the LdapIpAddress update, and then manually create the record that should be there. Here's a copy/paste of one of my previous posts to help you out:

=====

+++++

Actually most of these are strewn about in this newsgroup between myself and others posting responses. Steps include to kill the registration of your NIC cards thru the registry. You first identify the GUID for each NIC. Then you

## Re: AD DC registering private IP as AD DNS

would publish (thru reg) what IPs you want in DNS, then you need to adjust the binding order to insure the NIC you want to respond on. Then another reg entry to kill the GcIpAddress and the LdapIpAddress. Then you publish once again thru the reg which IP you want for those two values. But need to insure that the SRVs get registered properly., Then if RRAS is on it, it complicates it a bit. Then if this is also a NAT server, and you have multiple internal private interfaces, then there can be problems with routing between subnets because of the PDU size. LDAP requires a PDU or 300kb, but once enabled as a NAT, and you have multiple private interfaces, AD communication gets thwarted and requires another change. This can cause client logon trouble as well as GPOs to fail because of mutliple GC addresses come up, as they do on a multi homed DC/GC, then with round robin, you never know which one will answer and if it;s one on another subnet, then the system may not route it properly so therefore it can't get to it, even though the machine is on the same subnet.

Here's a repost of past posts I sent to explain some of it to others. They maybe mixed a bit, but you can see the jest of it. ALl the instructions are here to make it work. But it;s something you have to monitor to make sure it doesn;t cause any other issues. I've setup a couple machines thru this method, but it's a pain. If you had a member server doing this, (doesn't have to be an expensive box, just a cheapo desktop will do the trick), you would be better off.

~~~~~

Not saying it doesn't work with W2k3, but those articles are based on W2k.

The

registries are similar, but I know some of the registration entries on W2k have been changed on W2k3. Part of the issue you're seeing is with mutli NICs, when opening ADUC or any other domain requests, it maybe getting the wrong IP that is registered for the SRV resource. BTW– we always suggest to NEVER mutlihome a DC, DNS and especially never to put RRAS on it either.

Suggest

a member server for that. Or just get an inexpensive Linksys router to handle NAT.

But in many cases, I can understand that may not be possible in your environment.

Suggestions, and keep in mind, when mentioning "other NICs", they are the subnets that the NICs are on that your AD infrastructure is not on.

1. Insure that all the NICS only point to your internal DNS server(s) only and none others.

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).

Re: AD DC registering private IP as AD DNS

3. Disable NetBIOS on the other NICs (i know you did that thru the reg with that article, but insure that it's disabled in NIC properties too). May want to take a look at this to stop NetBIOS on teh RRAS interfaces:  
296379 – How to Disable NetBIOS on an Incoming Remote Access Interface [Reg Entry]:

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

Otherwise, RRAS or not, it will cause duplicate name errors because Windows sees itself with multi names thru the Browser service but with different IPs.

4. Disable File and Print services and disable MS Client on the other NICs. Uncheck reg this connection in DNS tab of IP properties/Advanced. Now if you need these for whatever reason for resource access from clients, then you would probably have to keep them on.

5. In DNS, delete the other NIC references for the LdapIpAddress – the blank domain FQDN – that looks like (same as parent). If this is a GC, you need to also stop the GC record as well.

To stop these from registering that info, use this method (this was taken from):

<http://support.microsoft.com/?id=295328>

=====

To disable only the registration of the local IP addresses, set the following registry value:

Key:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters

Registry value: DnsAvoidRegisterRecords

Data type: REG\_MULTI\_SZ

Values: LdapIpAddress

GcIpAddress

After you set this value, you must manually register your publicly available IP addresses for your domain to appear as:

Same as parent folder Host "publicIP" DO that by just rt-clicking, new host, leave the hostname blank, and enter the IP of the internal NIC.

You need to also manually create the GcIpAddress as well, if this is a GC.

That would be under the \_msdcs.\_gc SRV record under the zone.

=====

6. In DNS, \_msdcs.gc, delete the IP addresses referencing the other NICs. I would follow this article to stop the GC records from the other NICs registering sine this is a major cause of concern for logons. You would need to manually create the GC entry of the internal NIC.

Restrict the DNS SRV resource records updated by the Net Logon service [including GC]:

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

Re: AD DC registering private IP as AD DNS

7. Since this is 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 (for W2K, but may work):

275554 – The Host's A Record Is Registered in DNS After You Choose Not to Register the Connection's Address:

<http://support.microsoft.com/default.aspx?scid=KB:en-us:275554>

~~~~~

In circumstances in which the list of IP addresses the DNS server listens to and serves is different from the list of IP addresses published (registered by the DNS Server service), use the following registry key:

~~~~~

Also, how to kill registration (per NIC) prior to setting the above publishing records:

246804 – How to Enable–Disable Windows 2000 Dynamic DNS Registrations (per NIC too):

<http://support.microsoft.com/?id=246804>

~~~~~

275554 – The Host's A Record Is Registered in DNS After You Choose Not to Register the Connection's Address [It still registers]:

<http://support.microsoft.com/default.aspx?scid=KB:en-us:275554>

~~~~~

=====

==  
Regards,  
Ace

Please direct all replies ONLY to the Microsoft public newsgroups so all can benefit.

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 Windows MVP – Windows Server – Directory Services

Paramount: What's up with taking Enterprise off the air??  
Infinite Diversities in Infinite Combinations.

=====

.



Re: AD DC registering private IP as AD DNS

- **References:**

- ◆ **AD DC registering private IP as AD DNS**

- ◆ From: ErMaC

- Prev by Date: **Re: Members of DNSAdmins group cannot update DNS**

- Next by Date: **Re: Need DNS For Dummies! Please help!**

- Previous by thread: **AD DC registering private IP as AD DNS**

- Next by thread: **Strange DNS Problem**

- Index(es):

- ◆ Date

- ◆ Thread