

# Re: DNS Problem

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2008-02/msg00157.html>

---

- *From:* "Ace Fekay [MVP]" <PleaseAskMe@xxxxxxxxxxxxxxxx>
  - *Date:* Thu, 14 Feb 2008 00:18:31 -0500
- 

In [news:erfddarBIHA.4344@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:erfddarBIHA.4344@xxxxxxxxxxxxxxxxxxxxxxxx),  
SPG <nomail@xxxxxxxx> typed:

Have Windows 2003 Server R2, Exchange 2003 Server, DNS and a DC all rolled into one Server. All workstations, WinXP SP2, have the primary DNS pointing to the DC (this is necessary for MS Outlook to access the Exchange Server). The secondary DNS points to our ISP's DNS server (incase our DC goes down we can still get to the internet). All workstations are registered in our DNS in both Forward and Reverse zones. Our ISP's DNS servers are in our Forwarders. We live on email and the internet.

Here is the problem:

We have a website hosted on the outside. It is the same name (ie., abc.com) as our Lan domain name. When pinging our domain name we get nothing. When using NSLOOKUP it points to our DC. Thus, IE cannot go to our website. Is there a way to solve our problem ?

Thanks,

Sam

First, I would like to address your DNS strategy. Numerous errors can be caused by this configuration. The Microsoft best practice, and what all engineers will tell you, the cardinal rule with AD is to never use a DNS server IP address on any machine (DC, servers and workstations) that does not host the AD zone name or have some sort of reference to it (stubs, conditional forwarding, secondary zone, etc). Reason is AD requires exclusive access to it's zone name on the DNS server. This zone stores numerous amounts of information for AD to function, as well as other applications that are directory-enabled and exclusively rely on active directory to work. One example of such an app is Exchange. If there wasn't a global catalog available, or a way to query where it is, Exchange will fail. AD stores all of Exchange's configuration information. Matter of fact when you use the Exchange System Manager, it is not communicating with Exchange. It's actually communicating with active directory's Configuration Container.

## Re: DNS Problem

I do not believe your ISP's DNS knows how to query your internal zone name if a client, Exchange or the DC itself were to query it asking where the GC service is running.

Plus another reason why not is the client side resolver service, which is the service on any machine – DC or workstation – that queries DNS and what to do with the answer. It will query the first in the list, but if that doesn't respond, it will remove it from the 'eligible resolver list' for 15 minutes and go on to the next. So say if the client happens to try to authenticate to AD in order to access a printer, and it's stuck on the ISP's, it will fail to connect.

Another best practice, besides making sure ALL machines only use the DC as DNS, including itself, is to configure a forwarder to your ISP within the DNS server properties (right-click DNS servername, properties, Forwarding tab). If not sure how, please read the following article. Besides, if the DC goes down, so will email, domain functions, etc. This is a worst case scenario and wouldn't matter to config your machines with the ISP's DNS. If you need, you can configure your own workstation to the ISP's during such a crisis in case you need outside communication to research the problem.

323380 – HOW TO Configure DNS for Internet Access in Windows Server 2003 (forwarding) :

<http://support.microsoft.com/?id=323380>

Here are some additional reading that explains in more detail of what I mentioned above including additional information.

825036 – Best practices for DNS client settings in Windows 2000 Server and in Windows Server 2003

<http://support.microsoft.com/?id=825036>

Common Mistakes When Upgrading a Windows 2000 Domain To a Windows 2003 Domain (whether it was upgraded or not, this is full of useful information relating to AD and DNS, among other info):

<http://support.microsoft.com/?id=555040>

Domain Controller's Domain Name System Suffix Does Not Match Domain Name:

<http://support.microsoft.com/?id=257623>

Clients cannot dynamically register DNS records in a single-label forward lookup zone:

<http://support.microsoft.com/?id=826743>

300684 – Information About Configuring Windows 2000 for Domains with Single-Label DNS Names

<http://support.microsoft.com/?id=300684>

As far as accessing your external domain in a same name in/out config, you have two choices:

Re: DNS Problem

## Re: DNS Problem

1. Create a www record under your zone, and provide the actual external IP of the website.
2. Delegate www under the zone and provide two nameservers hosting the external zone. Nslookup will help you find that or check with your registrar for the registered nameservers for the zone.

In either choice, you will be limited to ONLY using <http://www.domain.com>. Reason why is back to AD and it's DNS reliance. The (same as parent) A record is actually the LdapIpAddress (some refer to the blank domain name of a zone) of all DCs in a domain. In your case with the one DC, it is the IP of that DC. That is the record in a website scenario that is created to access it by <http://www.domain.com>. IN AD it is a necessary record for GPOs and other domain functions to operate. So you are limited in this area. However there is a work around. You can install IIS. Under the default website, configure a redirect to [www.domain.com](http://www.domain.com). All http calls to the DC's IP will redirect to www, which you will have had a record or delegation created to get to.

--

Regards,  
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 – Directory Services  
Microsoft Certified Trainer

Infinite Diversities in Infinite Combinations

.