

# Re: Domain authentication problem

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.networking/2008-01/msg00028.html>

---

- *From:* "Ace Fekay [MVP]" <PleaseAskMe@xxxxxxxxxxxxxxxxxx>
  - *Date:* Thu, 3 Jan 2008 20:41:31 -0500
- 

In [news:u3OW7FmTIHA.4360@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:u3OW7FmTIHA.4360@xxxxxxxxxxxxxxxxxxxxxxxx),  
Bill Grant <not.available@online> typed:

To add to what Phillip said, there is no way to get this working properly with the DC offline. If you have a domain, all machines, including the DC itself, should be using the AD-linked DNS. Using an external DNS might get you Internet access, but access to AD resources will fail. Only your local DNS has these records.

All machines should use the D-Link as default gateway but use the DC for DNS and DHCP. The local DNS should be set to forward to an external DNS. (Forwarding to the D-Link should work, or you can use the DNS of your ISP). The DC needs to be up and running at all times.

Bill and Phillip, I agree, this is a huge problem with many configurations that time was not taken to understand how AD works, from conception, planning, and implementing AD. Configuring DNS and DHCP alone counts for 80%–90% of AD problems where the administrators are providing the DC and their clients with the ISP's DNS address or some other DNS that does not host the internal private AD zone. All they have to do is point DNS on ALL machines in the domain to the DC, setup a forwarder, and be done with it. Configure Windows DHCP Option 006 with the DC's IP address and all will be happy. Otherwise as what I like to say, it cuts into their drinking time when problems arise from doing it otherwise. :-)

Another huge problem I believe the original poster should take into account is that I believe takes up 10% of AD problems (keep in mind these are my guesstimates based on what we've see in these newsgroups in the past 8 years – and this figure has been dwindling since AD came out due to increased awareness and education on how AD works) is an AD domain configured as a single label name ("domain" vs the required format of "domain.com"). Tough one with this design error. A rename is possible, but I have not seen a successful one yet especially if Exchange is involved. A migration or worse, a reinstall to a new domain properly named, will fix this biggy.

We all know the above scenarios will DEFINITELY cause authentication issues,

## Re: Domain authentication problem

replication issues, can't open ADUC or any other AD tool, the DC can't even "find" itself, etc.

Why does this occur? I usually say, and this is with all due respect to the original poster, is lack of preparation and education on AD in understanding how AD works. Simply plugging the CD into the drive and installing the OS, etc, is not the answer to providing a properly functioning AD. I can understand that many companies either lack the resources or refuse to offer the ability to send their employees to classes to learn this stuff. In the long run it will cost them more in support, headaches and downtime. A five day Microsoft course on AD (MOC #2279) for around \$1500 will do wonders. But I am NOT here to sell a course. Just stating this as a fact from my experience as a trainer and a consultant since the early 90's. Matter of fact, this type of thing keeps me in business providing billable time as a consultant. :-)

Also many times with these Linksys, Netgear, etc, routers, especially if the ISP service they have is giving them an automatic IP address on the WAN interface, takes on the ISP's DNS addresses. So when you implement DHCP on some of these routers (not all of them but I know there are many that do) they automatically use these external DNS addresses in the lease. I know the ActionTecs do this by default and you can't change them. PITA they are. The router manufacturers designed these low-end routers for mostly home/consumer use and were not intended for an AD infrastructure, but nonetheless, they are used. No big deal, the idea is to just disable DHCP on them and use Windows. On top of that, the BIG reason not to use DHCP on a router is in all the cases I've seen, their DHCP service does NOT support DHCP Option 081, which dictates DNS Dynamic Registration, which we all know is a necessary function of AD.

Here are some articles for the original poster to read, and anyone else out there reading this post. I hope it helps them to get on the right track with AD.

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

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

291382 – Frequently asked questions about Windows 2000 DNS and Windows Server 2003 DNS

<http://support.microsoft.com/?id=291382>

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

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

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

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

Permissions, groups, OUs and GPOs are a whole other ballpark ...

Re: Domain authentication problem

Re: Domain authentication problem

—

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

.