

## Re: Choosing DNS Name

**Source:**

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2005-02/1954.html](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2005-02/1954.html)

---

**From:** Todd J Heron (*todd\_heron\_no\_spam\_at\_hotmail.com*)

**Date:** 02/27/05

Date: Sat, 26 Feb 2005 23:56:06 -0500

There are different answers to this classic question and while these answers ultimately depend upon company preference, much of the direction will be based upon administrator experience. The three basic options outlined below are the most commonly given answers to the question, sometimes altogether and sometimes not. Some company networks use a combination of these options. When explaining it to a relative beginner asking the question, I usually see all three options laid out or at least mentioned in some form or the other.

All three approaches will have to take both security and the end-user experience into perspective. This perspective is colored by company size, budget, and experience of personnel running Active Directory and the network infrastructure (mostly with respect to DNS and VPN). No one approach should be considered the best solution under all circumstances. For any host name that you wish to have access from both your internal network and from the external Internet you need option 1, although it is the most DNS-intensive over time. If you do not select this option and go with option 2 or 3 only, consideration will have to be given to the fact that company end-users will need to be trained on using different names under different circumstances (based on where they are (at work, on the road or at home)).

Option 1: Same internal and external DNS domain name. The administrator(s) maintain entirely separate DNS implementations (no zone transfers, etc.), where the internal AD/DNS domain has manually configured static records (web, mail, etc..) to get to frequently used IP hosts in the public DNS zone of the same name (currently most likely provided by your ISP, unless you are a very large company). The private AD/DNS zone is protected inside the network perimeter and is used to support the internal AD. This is known as "shadow DNS", "split DNS", split-brain DNS, or split-horizon DNS.

**Advantages:**

- 1) Security. Each DNS zone is authoritative for the zone of that name so therefore the external DNS zone and internal AD/DNS zone will NOT replicate with each other thereby prevent internal company records to be visible to the outside Internet.
- 2) Short namespace. Users don't have to type in (or see) a long domain name when accessing company resources either internally or externally. Names are

"pretty".

Disadvantages:

- 1) Any changes made to the public DNS zone (such as the addition or removal of an important IP host such as a web server, mail server, or VPN server) must be added manually to the internal AD/DNS zone if internal users will be accessing these hosts from inside the network perimeter (a common circumstance).
- 2) VPN resolution is problematic at best. Company users accessing the network from the Internet will easily be able to reach IP hosts in the public DNS zone but will not easily reach internal company resources inside the network perimeter without special (and manual) workarounds such as maintaining hosts files on their machines (which must be manually updated as well everytime there is a change to an important IP host in the public zone), or they must use special VPN software (usually expensive).

For further reading on this option:

[http://www.isaserver.org/tutorials/You\\_Need\\_to\\_Create\\_a\\_Split\\_DNS.html](http://www.isaserver.org/tutorials/You_Need_to_Create_a_Split_DNS.html)

<http://homepages.tesco.net/~J.deBoynePollard/FGA/dns-split-horizon-common-server-names.html>

Option 2: Delegated subdomain. This is subdomain of the public DNS zone.

For example, externaldnsdomain.com and subdomain.externaldnsname.com.

Advantages:

- 1) Like Option 1, this method also isolates the internal company network but note this is at the same time a disadvantage (see below).
- 2) Better than Option 1, internal company (Active Directory) clients can resolve external resources in the public DNS zone easily, once proper DNS name resolution mechanism such as forwarding, secondary zones, or delegation zones are set up.
- 3) Better than Option 1, DNS records for the public DNS zone do not need to be manually duplicated into the internal AD/DNS zone.
- 4) Better than Option 1, VPN clients accessing the internal company network from the Internet can easily navigate into the internal subdomain. It is very reliable as long as the VPN stays connected.

Disadvantages:

- 1) While there is security in an isolated subdomain, there is potential for exposure to outside attack. The potential for exposure of internal company resources to the outside world, lies mainly in the fact that because when the public zone DNS servers receive a query for subdomain.externaldnsname.com, they will return the addresses of the internal DNS servers which will then provide answers to that query.
- 2) Longer DNS namespace. This may not look appealing (or "pretty") to the end-users.

The option is the recommendation from the Windows Server 2003 Deployment Guide. It states to the external registered name and take a sub zone from that as the DNS name for the Forest Root Domain

<http://www.microsoft.com/resources/documentation/windowsserv/2003/all/deployguide/en-us/default.asp>

Option 3:

Different internal and external DNS domain names. For example, dnsname.com and dnsname.local. The administrator(s) maintain external records on the external DNS servers, and internal records on the internal DNS servers.

Still re-wording my notes on this one. This option is usually best for beginners b/c it's the easiest to implement. But makes VPN resolution difficult (like option 1) and Exchange headers when examined closely will show the company internal AD name which looks unprofessional. You can use any extension you want here such as .ad, .int, .lan, etc...

--

Todd J Heron, MCSE  
Windows Server 2003/2000/NT

-----  
Note: I do not top-post or bottom-post so that my responses are always easy to read in this forum and the Google Archives. This posting is provided "as is" with no warranties and confers no rights.