

## Re: Setting up Windows Server / Active Directory / DNS for small business

**Source:**

[http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active\\_directory/2004-12/1457.html](http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2004-12/1457.html)

---

**From:** Enkidu (*enkidu\_at\_xyzcliffxyz.com*)

**Date:** 12/28/04

Date: Tue, 28 Dec 2004 13:30:17 +1300

On Mon, 27 Dec 2004 23:13:21 GMT, "Peter"

<p.allaire2@NOSPAMverizon.net> wrote:

>

>*I will describe the current setup and am looking for some input on what the  
>new setup should look like. Since it is a small business with very few  
>users, I'm not planning on "migrating" the NT 4.0 domain server to windows  
>2003, I'm planning on basically configuring the win2003 server as a new  
>domain and then having all the workstations join the new domain.*

>

That IS a migration. The other option is to *\*upgrade\** the current domain to 2003.

>

> *Any files*

>*(such as users' saved documents on the old NT server will either be burned  
>to CDs or temporarily moved to one of the workstations, and then eventually  
>moved to the new server once it is online. I'll just create the 10 or so  
>user accounts on the new server.*

>

Sounds good.

>

>*Current setup:*

>*[snip]*

> *- The DSL router has a built in firewall and also acts as a DHCP server and  
>DNS server*

>

It would be best to stop it doing this. Use the Win2003 services instead.

>

>*Possible new setup:*

> *- 1 Windows 2003 Server used primarily as a File/Print server  
> - It will also be the new DHCP server, and DNS server*

>

Ah, good.

>

>*Its possible that sometime in the future we may decide to host our own*

>website and email, ideally it shouldn't require a network redesign to  
>accommodate that.

>

The router may be able to support a DMZ setup, where the Web server is effectively on a separate network to the LAN. I'd investigate that. If not, I'd look for a device that *\*will\** allow it. You *\*could\** punch a hole in the firewall and have the web server on the LAN, but that opens up a bag of worms. If you can't keep the web server separate from the LAN, you could get it hosted elsewhere and still maintain it and have complete control. Check your local (and remote!) service providers.

For the email, you will either have to punch a hole in the firewall or host the mail server on a DMZ. Are you sure that you want the hassle? You will have to configure the mail server to filter viruses and SPAM and generally keep it up to date with SPAM and virus defs. It is potentially a lot of work.

>

>*My biggest questions are about the domain structure and what the domain should be called.*

>

>*Should the new domain name be called SUNRAYVT.COM or SUNRAY.SUNRAYVT.COM?*

>*Or should we register a completely new public domain name? Even though we*

>*own the sunrayvt.com public domain, it is being used by the ISP that we*

>*chose to host the website and email, so I'm not sure if it can also be used*

>*by us for our windows domain.*

>

>*If we did use sunrayvt.com, I'm assuming the workstations would be named*

>*something like workstation1.sunrayvt.com, workstation2.sunrayvt.com, etc.*

>>*From a workstation on our network, how would we be able to get to*

>*www.sunrayvt.com, since it's not actually a computer in our network? Is*

>*there some sort of DNS setup that I would need to do to tell traffic for*

>*www.sunrayvt.com to go to a certain external IP address?*

>

There are many schools of thought on this one, and many of the debates flare into almost religious wars. Simple answer is to choose what seems to you the best way to go. I've run systems where the LAN Domain name was the same as a registered Domain Name, where the LAN Domain Name was a sub-Domain of a registered Domain Name and where the LAN Domain Name was a bogus Domain Name eg "cliffs.lan".

I've not found too many operational issues with any of them. You will have an internal DNS and you will have an external Internet DNS to interact with. If the LAN Domain Name is the same as your Internet Domain Name, then you in essence need to set things up as follows:

1) All clients including the DNS servers have to be configured via DHCP or manually to reference the DNS internal servers *\*only\**

2) The internal DNS servers NICs need to be configured to reference themselves as DNS.

3) The gateway for \*all\* machines is the ADSL router.

4) The DNS service on the DNS servers needs to be configured to forward all requests it doesn't know about to an external DNS, eg your ISPs. These are the only machines that talk to an external DNS.

So far the applies to all AD setups. If your LAN Domain Name is the same as your Internet Domain Name then you have to do the following:

5) Manually add an external machines that yuse your common Domain Name to DNS. eg if www.company.com exists outside the LAN and you need to access it from inside the LAN, add www.company.com manually to the DNS with its correct IP address. Since the IP address is external, packets to the server will go out the gateway/ADSL router to the right place.

>

>*Any input you can provide regarding my questions or other setup tips for*

>*small businesses would be appreciated. Please also let me know if you know*

>*of any resources for setting up windows 2003 in a small business*

>*environment.*

>

www.microsoft.com !! <grin> Seriously that is a good place to start.

There are also courses and books and other websites.

Cheers,

Cliff

{MVP Directory Services}

--

The National Party manifesto can be viewed here:

<http://www.labour.org.nz/policy/index.html>