**NE259 – Windows Server – Lab6**

**Points deducted if All Answers Are Not In: Ariel, 14pt, Bold, Red!**

In this lab you will examine the configuration of DNS on a server and use that server to provide DNS services for a client computer.

Required Materials:

**SRV16** and **WIN10** images prepared in previous lab exercises.

DNS

DNS is used on all modern networks and the Internet. It provide the mechanism for converting names such as www.google.com into IP addresses. DNS is also critical to the operation of Active Directory. Without a well-functioning DNS system, Active Directory will not work. Many problems encountered with working with servers and Active Directory are essentially DNS problems which cause other problems such as the inability to authenticate (log on) or connect to network resources and the Internet. Computers in an Active Directory forest use DNS to locate domain controllers and other network resources.

You can manually configure DNS or you can let the promotion process perform a basic DNS installation and configuration with creating the first domain controller in a domain. You already did this in a previous lab exercise although you might not have been aware of it at the time.

DNS can provide two different kinds of DNS name resolution. In what is called a Forward lookup, a domain name resolved to an IP address. This is the most common type of DNS function. DNS can also provide a Reverse or Inverse lookup by resolving and IP address to a name. This is far less common and not normally needed. Reverse lookups don’t work on the Internet, but can have some utility in a local network.

Typically, a client computer (like a network workstation) sends a DNS Query to a DNS server that requests a name to be resolved. The DNS server then responds with a DNS Query Response that either provide the IP address or informs the client that the name cannot be resolved (doesn’t exist).

Client computers store the results they receive from a DNS server in a temporary memory cache, called the Resolver Cache, so that subsequent queries for the same name don’t generate additional network traffic and load on the DNS server.

Part 1: Examine the DNS configuration for your Domain

In Lab 2 you promoted **SRV16** to be a domain controller in the AVERY.pri domain so DNS was already installed and configured on your server. In the next steps you will examine the results of that action.

* Start **SRV16** and logon with your personal account.
* From the Tool menu of Server Manager select DNS
* Expand the **SRV16** icon in the DNS module. You should see four to five containers under **SRV16**. List them below.

**Forward lookup zones**

**Reverse lookup zones**

**Trust points**

**Conditional forwarders**

* Expand the Forward Lookup Zones container. You should see two Forward Lookup zones. Record them below.

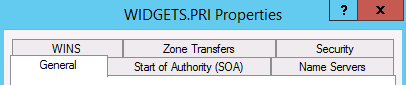
**\_msdcs.AVERY.PRI**

**AVERY.PRI**

* Expand the A VERY.pri forward lookup zone

In the right pane you will see subfolders and some standard DNS records. Under the Type column you will see the record types. You should see Host (A) records for both **SRV16** and **WIN10**. (These DNS names are not case sensitive.) These are the records used to allow DNS to resolve the names like **SRV16**.AVERY.pri and **WIN10**.AVERY.pri to their respective IP addresses.

* Right click on the AVERY.PRI forward lookup zone icon in the left pane and select Properties from the menu.
* With the General tab open examine the screen and record what you see below:



Status **Running**

Type **Active Directory-Integrated**

Replication **All DNS servers in this domain**

Dynamic Updates **Secure only**

* Close the properties window.

Part 2: Create a Reverse Lookup Zone

* Left click on the Reverse Lookup Zones container in the left pane of the DNS Manager. You should not find any zones present. [There are three hidden zones, but those are not of interest to us at this point.]
* Right click on Reverse Lookup Zones.



* Click Next to get to the Zone Type window. You will see one radio button selected and a check box.

What Zone type is selected with the radio button? **Primary Zone**

Where will the zone information be stored? **Active Directory**

A DNS Primary zone is a zone that can be updated manually or by dynamic updates from other computers. There are two types of Primary Zones, Standard and Active Directory Integrated. With Standard Primary zones, there is one DNS server that has a writable copy of the zone information. With Active Directory Integrated zones, every DNS server with that zone is writeable. Active Directory Integrated zones are the preferred zone type for supporting Active Directory domains.

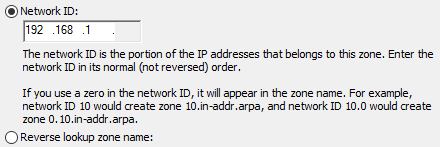
* Leave the default selections and click the Next button. Since you have selected to make this an Active Directory Integrated Primary zone you can select how changes in the DNS zone will be replicated (copied) to other computers. You will accept the default choice.
* List the default choice for replication of this new zone, then click Next

**To all DNS servers running on domain controllers in this domain: AVERY.PRI**

* Although DNS can work with both IPv4 and IPv6, we will make this an IPv4 zone.



* For the zone name you will input the Network ID of your private network. Notice that as you type in the Network ID, the zone name below will automatically change and reverse the IP address.



What is the Reverse Lookup zone name?

1.168.192.in-addr-arpa

* At the Dynamic Update window leave the default radio button selected.

Which Update Type was selected?

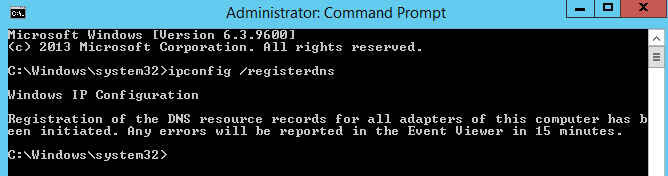
* + **Secure Only**
  + Non-Secure and Secure
  + Do Not Allow Dynamic Updates
* Click **Next** then **Finish**.
* Left click on the new Reverse Lookup Zone and then record the Type of the two records you see in the zone in the right pane.

**Start of authority**

**Name server**

Next you will have your two computers register themselves in the Reverse Lookup Zone. You could reboot them, but there is a quicker way.

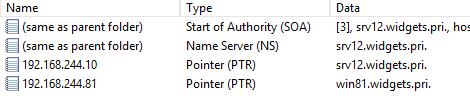
* Open an **Elevated Command Prompt** (right click on the Command Prompt icon and select Run as Administrator. You will need to accept the User Account Control query by clicking on Yes with prompted.
* At the command prompt issue the command  **ipconfig /registerdns**



* Close the command prompt and click on the Refresh icon in the DNS Manager



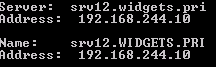
* You should now see the Pointer (PTR) record for **SRV16**.
* Log onto **WIN10** with your personal account, open an Elevated command prompt and use the **ipconfig /registerdns** command to force **WIN10** to register.
* Return to **SRV16**, refresh the DNS display and you should now see both entries in the Reverse Lookup zone. (Don’t continue until you can see both.)



Part 3: Send a Query to a DNS server

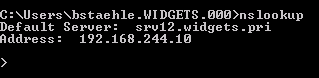
In the next section you will use the NSLOOKUP command to send a query to a DNS server and receive a response. The NSLOOKUP program only waits 2 seconds for the DNS server to respond before giving an error message, so sometimes it is necessary to send a query more than once. This can be cause by a slow network or a busy DNS server. Commands with NSLOOKUP are not case sensitive.

* Switch to **WIN10**
* If you don’t have a command prompt open, open one now. It does not have to be elevated.
* Issue the command **nslookup SRV16**
* The response you get will be in two parts. The top two lines give you the name and IP address of the DNS server that you sent the query to. The last two lines are the response that came back from the server.



NSLOOKUP can also be used in interactive mode. In this case you will issue the command nslookup without a name to query and you will get > symbols where you can type in a query. Once that query in answered you will get the chance to ask another question without typing our nslookup again. To exit the NSLOOKUP command and return to a normal command prompt you can issue the EXIT command or just close the command prompt box.

* Issue the command **nslookup**
* You will see the name and address of the DNS server that will be answering your questions. You can now enter name for a query at the > prompt.



* Enter the name **WIN10**
* Did the name resolve correctly? **[ Y / N ] Y**
* In the two queries you have issued so far, your DNS server was able to answer the questions from its AVERY.pri zone file. However, your DNS server is capable of lookup up other names by going out to the Internet and searching for them.
* Issue the command www.neit.edu at the nslookup > prompt. If you get DNS Request timed out, just hit the up arrow on the keyboard to repeat the query.

What is the IP address for www.neit.edu? 216.15.173.27

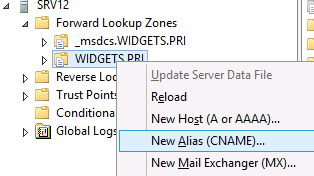
Some DNS names are associated with more than one IP address. This is normally done for load balancing and is called DNS Round Robin.

* Lookup [www.amazon.com](http://www.amazon.com) at the > prompt.
* How many IPv4 IP addresses do you get? **Three**
* Try looking up some Internet domain names to see how NSLOOUP works.
* When you are done using NSLOOKUP type EXIT at the > prompt. *(It isn’t case sensitive. Upper case letters are used here just for emphasis.)*

Part 4: Create an Alias Record

DNS allows you to have more than one DNS name for the same IP address. This is called an Alias or CNAME record.

* .Switch back to **SRV16**
* In the DNS Manager, right click on the AVERY.PRI domain name and select New Alias.



* In the Alias Name field type in your first name and notice that the field below, Fully Qualified Domain Name is automatically adjusted for the name you entered.
* For the Fully qualified domain name of the target host enter **SRV16.AVERY.pri** and then click OK
* Examine the record you have just created.
* Switch to **WIN10**
* Open a command prompt if one isn’t open already and issue the command nslookup followed by your first name. The output should show the real computer name and IP address of the computer for which you created the alias.

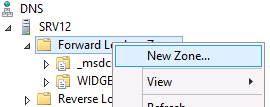
Continue on to Part 4

Part 4: Importance of the Zone file

When a DNS server is present with a query (asked a question) the first place it looks for the answer is in zones. If the DNS server holds a zone that matches the query, it will answer the query from the contents of the zone. This is true whether the zone has the requested information or not. If it does not have the requested information in the zone file, it sends back a negative response (name could not be found). A DNS server will never check anywhere else for the answer if it has a zone file that matches the query.

In the next steps you will create a zone file in your DNS server and see how this works.

* In **SRV16**, open the DNS Manager.
* Right click on the folder that holds the Forward Lookup Zones and select New Zone from the menu.



* Click next and examine the choices you have for creating a zone. For this exercise you will create an Active Directory Integrated zone. The defaults for this should already be selected. The radio button for Primary Zone only means that this zone file will be writable. The check box at the bottom of the screen determines whether this will be a Standard or an Active Directory Integrated zone file. If the box is checked the zone file is stored in the Active Directory data base (NTDS.DIT). If the box is not checked, the zone will be a Standard Primary zone and the zone file will be stored as a plain text file on the hard drive.

Is the default a Standard Primary or AD Integrated zone?

**AD integrated.**

* Click Next to get the screen that determines how the zone file will be replicated in your Active Directory network. (You would not get this choice if you had selected a Standard Primary zone file.

What is the default setting for replication of the zone file?

**To all DNS servers running on domain controllers in this domain: AVERY.PRI**

* Click Next and you will be taken to the Zone Name dialog box.
* Give the zone the name bigbiz.com and click Next.
* You should now be at the Dynamic Update windows in the wizard. Since this is a test zone, we could really answer anything here. In this case, select the radio button for **Do not allow dynamic updates**. This will require manually configuring of any names that the zone will look up. This choice is normally reserved for testing and not a viable option for a real zone supporting an Active Directory domain.



* Click on Next and then Finish at the next screen to complete the creation of the zone.
* Under the Forward Lookup Zones folder, left click on the new bigbiz.com domain name and examine the only records that have been created. You will see that there are no Host records

Name Type

**(same as parent folder) State of authority**

**(same as parent folder) Name Server**

* Now switch to the **WIN10** image
* Open a command prompt and issue the command: **nslookup** [**www.bigbiz.com**](http://www.bigbiz.com)



What message do you get? (The message will begin with **\*\*\***.)

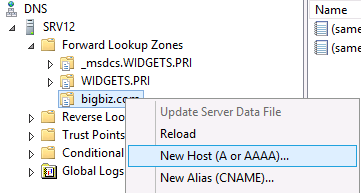
**\*\*\* SRV16.AVERY.PRI can’t find this domain:** [**www.bigbiz.com**](http://www.bigbiz.com)**: non-existent domain**

* Now issue the command: **nslookup bigbiz.com** *(Leave off the www)*

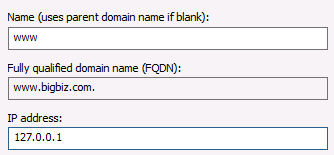
What message do you get?

**Server: SRV16.AVERY.PRI address: 192.168.1.45**

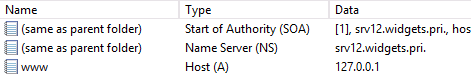
* Return to **SRV16**
* Right click on bigbiz.com and select New Host (A or AAAA).



* For the Name field, type in www.
* For the IP address type in 127.0.0.1



* Leave the check boxes bland and click on Add Host. Then click through to get back to the DNS manager and examine the new host record.



* Return to **WIN10** an issue the command **nslookup bigbiz.com** as you did before.
* Record the results below.

**Server: SRV.16.AVERY.PRI**

**Address: 192.168.1.45**

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Open you IE browser on **WIN10** and put [bigbiz.com](http://www.bigbiz.com)

Where does the browser take you *or what message do you get?*

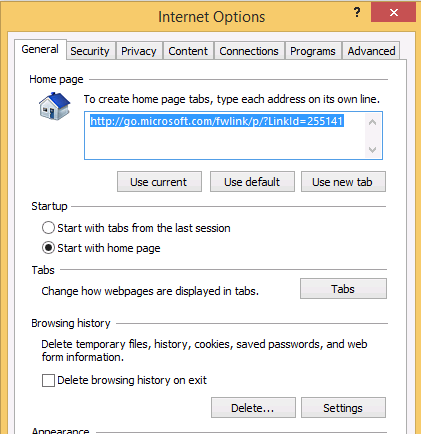
**“This page can’t be displayed”**

* Close the browser and return to **SRV16** and to the DNS Manager.
* Right click on the bigbiz.com zone name and select Delete from the menu. Accept the defaults to actually delete the zone.
* Return to **WIN10** an issue the command **nslookup bigbiz.com** as you did before.
* Record the answer under Non-authoritative answer:

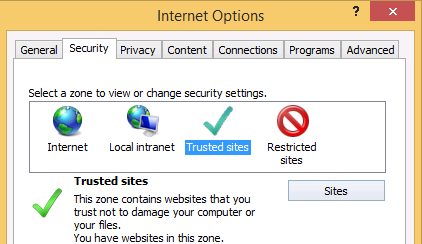
Name: **bigbiz.com**

Address: **216.218.198.8**

* There really is a domain called bigbiz.com on the Internet. However, if your DNS server had a dummy zone for bigbiz.com, you would not be able to get to it through DNs.
* Open your browser and clear the browser cache
  + Click on the gear icon in the top right corner of the browser
  + Select Internet Options then click the Delete button (as shown in the following screen shot.)



* After deleting the browser cache, try to go to [bigbiz.com](http://www.bigbiz.com) by putting the URL in the browser.
* If you get the message “This page can’t be displayed” it shows the DNS is working but the added security features of IE are preventing the browser from displaying the site. To get around this, you can add [bigbiz.com](http://www.bigbiz.com) to the list of Trusted Sites using the following steps
  + Go to Internet Options in the browser
  + Click on the Security Tab then click on the green check mark for Trusted Sites
  + Click on the Sites button and add <http://bigbiz.com> to the trusted site list.





* Now try to get to [bigbiz.com](http://www.bigbiz.com) with the browser, it should work.
* Stop and show the instructor the bigbiz web site. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Instructor’s initials

* When completed, shut down both images normally.

-END