# Windows Server – Setup and Configuration

# Section 4 – Network Services (DNS)

Machines:

* 1 Windows Server 2016
* 1 Windows 10 Client Machine

## Part 1: Windows Server DNS Configuration

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.

* Start your server and logon with your personal account.
* From the Tools menu of Server Manager select DNS
* Expand the SRV16 icon in the DNS module. You should see four to five containers under your server.
* Expand the Forward Lookup Zones container. You should see two Forward Lookup zones. Record them below.
* Expand the domain 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 your server and your client. These DNS names are not case sensitive. These are the records used to allow DNS to resolve the names like **<servername>**.<domainname>.com and **<clientname>**.<domainname>.com to their respective IP addresses.

* Right click on the WIDGETS.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:

Graphical user interface, text, application, chat or text message

Description automatically generated

Take note of the following settings:

Status

Type

Replication

Dynamic Updates

## Part 2: Reverse Lookup Zones

* 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 actually three hidden zones, but those are not of interest to us at this point.]
* Right click on Reverse Lookup Zones.

Graphical user interface

Description automatically generated with medium confidence

* 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?

Where will the zone information be stored?

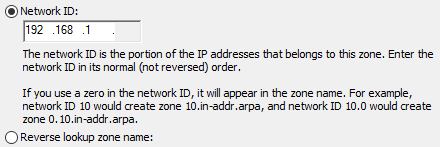
By definition, a DNS Primary zone is a zone that can be updated manually or by dynamic updates from other computers. There are two types of Primary Zones, Standard and Active Directory Integrated. With Standard Primary zones, there is one DNS server that has a writable copy of the zone information. With 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 are allowed to select how changes in the DNS zone will be replicated (copied) to other computers. You will accept the default choice.
* Leave the default choice for replication of this new zone, then click Next
* Although DNS can work with both IPv4 and IPv6, we will make this an IPv4 zone.

Text

Description automatically generated with low confidence

* 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.



Take not of the Reverse Lookup zone name.

* At the Dynamic Update window leave the default radio button selected. Take note of this default.
* Click Next then Finish.
* Left click on the new Reverse Lookup Zone and then take note the Type of the two records you see in the zone in the right pane.

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**

Text

Description automatically generated

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

Graphical user interface, application, Teams

Description automatically generated

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

Graphical user interface, text, application

Description automatically generated

## Part 3: DNS Queries

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 the client
* If you don’t have a command prompt open, open one now. It does not have to be elevated.
* Issue the command nslookup <servername>
* 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.

Text

Description automatically generated

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.

Text

Description automatically generated

* Enter the **<clientname>** to verify the name resolves.
* Issue the command www.google.com at the nslookup > prompt. If you get DNS Request timed out, just hit the up arrow on the keyboard to repeat the query.

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

* Try looking up some Internet domain names to see how NSLOOKUP 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 3: Alias Records

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 **your server**
* In the DNS Manager, right click on the domain name and select New Alias.

Table

Description automatically generated

* 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 **<servername>.<domainname>.com** and then click OK
* Examine the record you have just created.
* Switch to **the client**
* 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.

## Part 4: The Zone File

When a DNS server is presented 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 **the server**, open the DNS Manager.
* Right click on the folder that holds the **Forward Lookup Zones** and select **New Zone** from the menu.

Graphical user interface, application

Description automatically generated

* 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.

Take note of the default zone type.

* 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.

Take note of the default setting for replication of the zone file.

* 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
* Now switch to the **client**.
* Open a command prompt and issue the command: **nslookup www.bigbiz.com**



Take note of the message you get vs the message you get after the next command:

* Now issue the command: **nslookup bigbiz.com** *(Leave off the www)*
* Return to **the server**
* Right click on bigbiz.com and select New Host (A or AAAA).

Graphical user interface, application, table

Description automatically generated

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

Graphical user interface, application

Description automatically generated with medium confidence

* 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.

Graphical user interface, text, application

Description automatically generated

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

**Server:**

**Address:**

**Name:**

**Address:**

* Open you browser on **your client** and enter the www.bigbiz.com address.

Take note of the message you get.

* Close the browser and return to **the server** and to 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 **the client** an issue the command **nslookup www.bigbiz.com** as you did before.
* Take note of the answer under Non-authoritative answer:
* There really is a domain called bigbiz.com on the Internet. However, as long as 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
* After deleting the browser cache, try to go to **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

Graphical user interface

Description automatically generated

Icon

Description automatically generated with low confidence

* Now try to get to bigbiz.com with the browser, it should work.