Lab 3 DNS and Name Resolution

Part 1 Examine the **HOSTS** file and **Resolver Cache ON CLIENT1**

Every Windows computer maintains a HOSTS file. The contents of the HOSTS file are loaded into the client's Resolver Cache when the computer boots up. **Any time the contents of the HOSTS file change, the Resolve Cache is updated accordingly**. Since **the Cache is always examined before the client contacts a DNS server, information in the HOSTS file can prevent unnecessary DNS lookups saving time and reducing network traffic.** However, incorrect entries (intentional or accidental) in the HOSTS file can cause a client to be directed to an invalid location. The HOSTS file is also used by anti-malware software to prevent the client from locating known malicious or undesirable sites.

**To help protect critical Windows files such as the HOSTS file from malicious attack, the Windows directory and sub directories are given additional access protection.**

In addition to the contents of the HOSTS file, the Resolver Cache maintains a list of recently resolved names to avoid repeated queries to the DNS server. Examining the Resolver Cache will show both recently resolved names as well as the contents of the HOSTS file.

In addition to the Resolver cache maintained by the client, Web browsers also maintain a cached of recently accessed site. Changing the HOSTS file will change the contents of the Resolver Cache, but not the Browser caches. A Web browser will check its own cache before requesting resolution from the DNS client service.

* + 1. Log into CLIENT1 and open an elevated command prompt. In the Command Prompt, navigate to the {***systemroot****}*\**system32\drivers\etc** folder. *(Hint: you will need to use the CD command.)*
    2. Flush the resolver cache with the following command

**ipconfig /flushdns**

* + 1. Display the flushed DNS Resolver Cache by issuing the command:

**ipconfig /displaydns**

**What message do you get? \* “Could not display the DNS Resolver Cache”**

Although this looks like an error message, it just means that the resolver cache is empty.

* + 1. Open the {***systemroot****}*\**system32\drivers\etc**\HOSTS file in Notepad by issuing the command: **notepad hosts**.
    2. You should see entries for Local Host, one for IPv4 and one for IPv6. Activate them by removing the # symbol in front of the lines they are on.

*Note: Any lines that begin with the # symbol are considered comments and are not used.  
Modify as shown below.*

|  |
| --- |
|  |

* + 1. Save, but DO Not Close the notepad changes and minimize Notepad with the HOSTS file.
    2. Examine the DNS Resolver Cache again (**ipconfig /displaydns**). You should see a number of different entries. These should be IPv6 and IPv4 reverse lookup and forward lookup entries.

|  |
| --- |
| Screenshot: |

* + 1. In the Command Prompt, clear the Resolver Cache with the command:

**ipconfig /flushdns**

* + 1. Run ipconfig /displaydns again

**Did the hosts file information get flushed from the resolver cache? [ Y / N ] N**

* + 1. Minimize the Command Prompt, open **Microsoft Edge** or **Chrome** and go to **www.google.com**.
    2. Configure Edge or Chrome to use this URL as the default home page then close the browser.

|  |
| --- |
| Edge home page set. |

* + 1. Run ipconfig /displaydns for a list of current resolver cache content.
    2. Now flush the resolver cache one more time.
    3. Open IE and after it goes to Google, examine the DNS Resolver Cache again (**ipconfig /displaydns**). You should see a number of different entries. Note that not all the entries have the same TTL.

**Where do the Time to Live (TTL) values for the** [**www.google.com**](http://www.google.com) **entries come from?\* They come from the name server machine(s) for google.com**

* + 1. Select one of the **www.google.com** entries and detail it here.

Record Name: **www.google.com**

Record Type: **1**

Time to Live: **30**

Data Length: **4**

Section: **Answer**

A (Host) Record: **172.217.12.228**

* + 1. Run ipconfig /displaydns again and you should see the TTL is smaller now

**What is the new TTL? 23\***

* + 1. Clear the DNS Resolver cache (**ipconfig /flushdns**)

# Part 2 - Active Directory and DNS

1. On DC1 open the DNS Tool from the Server Manager
2. Drill into the NE381JK.COM domain to the Forward Lookup Zones folder

On the right you should have two forward lookup zones

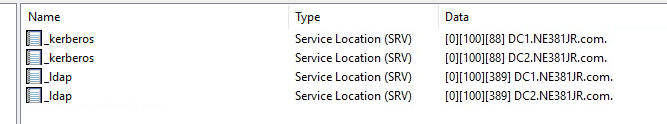
These were created automatically when you installed Active Directory in the Server.

|  |
| --- |
| Snip the zone records: |

1. Click on the first Forward Lookup Zone it should look something like this.



This forward lookup zone looks much different than any other forward look up zone. In an Active Directory (AD) domain, the \_msdcs DNS zone stores several types of resource records pertaining to domain controllers (DCs). If this zone is not present or not functioning properly, domain members may not be able to locate a DC and thus may not be able to access resources in the domain. To accommodate locating domain controllers by server type or by GUID (abbreviated "dctype"), Windows Server domain controllers register SRV records in the following form **\_Service.\_Protocol.DcType. \_msdcs. DnsDomainName.** Here are what some of the records look like.



1. There should be a total of four main folders under the \_MSDCS zone file.  
   **What are they and what are the names short for?\***
   1. **Dc (Domain Controller)**
   2. **Domains (domains)**
   3. **Gc (Global Catalogs)**
   4. **Pdc (Primary Domain Controller)**
2. Drill into domains à GUID à \_tcp the tree will look something like this.



1. Note what SRV is short for. These records are SERVICE LOCATION or LOCATOR Records.

|  |
| --- |
| **Screenshot the two server records that appear in the right panel.** |

**What is the purpose of these two records based off of the container object and the name of the record?\***

**To allow machines in a domain to locate domain controllers.**

1. Collapse the MSDCS zone file
2. Click on the zone file folder for the NE381*XX*.COM domain

You should see the right-hand pane populate with Multiple entries. The records on the right that state *(****same as parent folder)*** mean that they will have the same name as your zone file.

**What is the name of the Start of Authority (SOA) record for your domain? \* “(same as parent folder)” which is NE381WB.com**

A Start of Authority Record or (SOA) is typically used to signal what DNS server is authoritative for a zone. This is used when the DNS infrastructure is setup as Master/Slave or Primary/Secondary. The setup in the lab is Active Directory Integrated meaning all the zones are stored in the AD database. Each DC that hosts DNS is authoritative for itself.

1. Right click on your NE381XX.COM zone folder and go to properties. Note the Type is Set to Active Directory-Integrated and changes are replicated to all DNS servers in the Domain.
2. Double check to **ensure that Dynamic updates are set to secure only.**
3. Click on the Start of Authority (SOA)

**What is the SOA Primary Server for the DNS server on DC1? Dc1.ne381wb.com**

Click the **Name Servers** tab this will show (should show) all DNS servers in the domain. If a server does not belong here it should be removed. If any servers are not in this tab that are AD DNS servers they should be added.

|  |
| --- |
| **Screenshot your servers in the Name Servers Tab\*** |

1. Close the properties box and make sure you have NE381XX.com zone file selected.



On the right you should see multiple records. Two of these records are Host (A) records that say (same as parent folder). These records have the same ip addresses as the two domain controllers in the domain. Each domain controller in the domain will have an entry like this. This allows for a user/computer/system to be able to ping a domain name and get a response back from a domain controller. The domain controller oversees the domain. Stale or dead entries in this section can adversely affect domain operation.

1. Log on to CLIENT1 and ping your domain name.  
   **What IP results were returned? \***

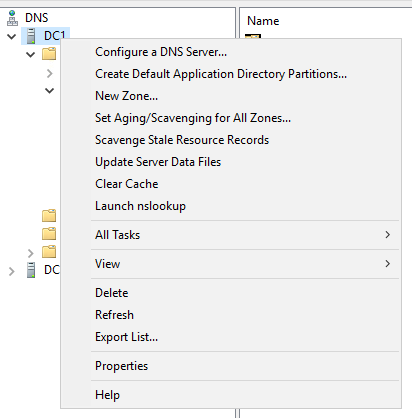
|  |
| --- |
| Snip of result: |

1. Log to CLIENT2 and ping your domain name.  
   **What IP results were returned? \***

|  |
| --- |
| Snip of result: |

The two clients should have returned two different IP results. Each client should be contacting the domain controller that is logically closer to it if the service queried is not AD site enabled. The DNS server will force the DNS server on the same network to respond. The following article is a good resource for how this works <https://technet.microsoft.com/en-us/library/cc961422.aspx>

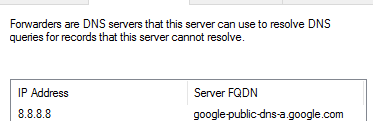
1. Temporarily Suspend DC1 **using the Skytap button**, wait a few moments then ping your domain name again.  
   **What results were returned and what does this tell you? \* “Destination host unreachable”, CLIENT1 is pinging the domain using the IP of the DC logically closest to it which is currently down. This tells me CLIENT1 only has one IP to use to contact the domain.**
2. Resume DC1 wait a moment and then attempt a ping from CLIENT1 again. You should see DC1 server ip address respond. If you do not then something is wrong.
3. From DC1 within the DNS management tool right click on DC1 and select properties.



This is where settings specific to the DNS server are stored.

Under the interfaces tab make sure that All IP Address is selected. For our configuration this is acceptable. Since we only have two network addresses. Both addresses listen for DNS requests locally.

1. Click on the forwarders tab. You should see 8.8.8.8 here. This setting was migrated over when DNS was installed. IF you do not see this setting [Edit] and add it now.



Forwarders are used when a DNS server cannot locate a record for a given query. It will take the query and forward it to the specified server.

1. Click on the **[Advanced]** tab and you should notice that the **Disable recursion check box is not selected.** This is a good thing. Without recursion then queries for names could take a lot longer. Since we are on an internal network we can leave this unchecked to speed up queries. If we were hosting a public DNS server we may want to check this setting to prevent DDOS DNS attacks.
2. Close out of the properties dialog box.
3. Locate the Reverse Lookup Zone folder and click on it. You will notice that there are no reverse lookup zones. These are not created by default and need to be added.
4. Right Click on the **Reverse Lookup Zones** folder and Select New Zone.

Click Next and select **Primary Zone**. Also take note that the following check box is selected.  
**What are the other two zone choices? \* Primary, Secondary, and Stud zone**



1. Keep the default to all DNS servers running on domain controllers in this domain.
2. Select IPv4 Reverse Lookup Zone
3. Under Network ID enter the network for the DC1 server. Make sure to read the full dialog on this prompt.  
   **What is the Network ID for DC1? 192.168.1**
4. Select **Allow Only Secure Dynamic Updates** then finish
5. Repeat this process for DC2 network.  
   **What is the Network ID for DC2? 10.0.0**

**At the end we should have two reverse lookup zones created. Screenshot the two reverse lookup zones for submission to canvas\***

|  |
| --- |
| **DC1:** |
| **DC2:** |

Reverse Lookup Zones will resolve ip to names. Which is the opposite of the forward lookup or standard dns query. These records are also called PTR records.

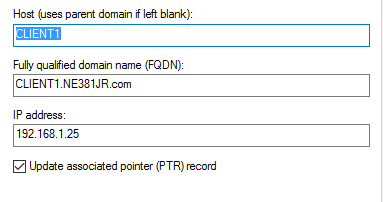
1. Navigate back to the Forward Lookup Zone NE381XX.com
2. Now, return to DC1 and open a new command prompt and ping your client1 IP. **If you get a request timed out set the CLIENT1 firewall to allow** **‘File and Printer Sharing (Echo Request – ICMPv4 In) for the Domain.**  
   **Do not turn the Firewall Off!**

|  |
| --- |
| **Snip showing proper configuration of Firewall to allow ICMP Ping packets:** |

1. Now ping again and this time put -a before the ip address.

The -a is telling to resolve the name during the ping. This should yield no results because we do not have a pointer record created for CLIENT1 yet.

1. Back in the DC1 -> DNS -> NE381XX.COM record folder, Double click on the CLIENT1 A record and put a check in the Update associated pointer record.



This will create the pointer record in the reverse lookup zone for this network. Navigate to this zone to verify the creation.

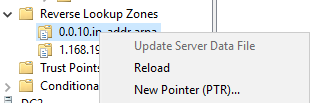
1. From a DC1 command prompt run **ipconfig /flushdns**
2. Now ping the ip address again with the -a switch again



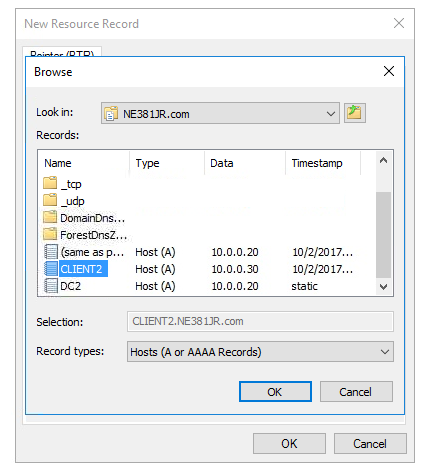
**You will see that the name is resolved on the first line of the response.**

|  |
| --- |
| **Screenshot your results for upload to canvas. \*** |

1. Reboot DC1 & DC2 the log back into each using your personal Administrative account.
2. In the DC1 -> DNS management tool click on the 0.0.10.in-addr.arpa zone to select.
3. Right click on the zone and select New Pointer (PTR)



1. Click on Browse and Drill into DC1 until you locate the CLIENT2 IP. Select this record and Click OK and finish creating the record.



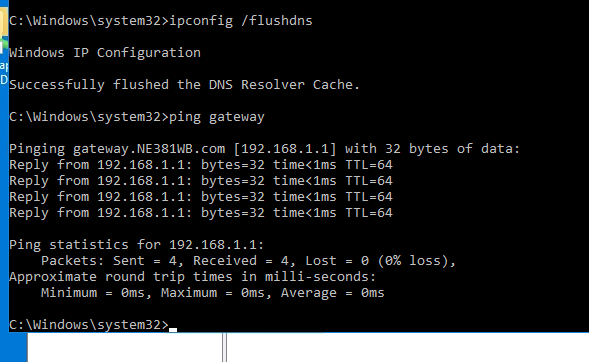
Drill into the Reverse Lookup Zones 0.0.10.in-addr.arpa zone folder and you should see a new PTR. Make sure you see the time stamp static set. If you do not click the refresh button in the management tool.



|  |
| --- |
| **Screenshot this entry for submission to canvas\*** |

1. From a DC1 command prompt type **ping gateway**
2. What happened? **“Could not find host gateway” .. This is because there is no “gateway” host record.**
3. Right click on the NE381XX.COM zone folder and select new host A or AAAA.  
   If an A record is for a standard ipv4 address…  
   **What does AAAA stand for? \* AAAA refers to ipv6 as opposed to A (ipv4)**
4. For the name enter in gateway and give it an address of 192.168.1.1
5. From a command prompt type **ping gateway**.  
   What happened now?

**Screenshot these results and save for upload to canvas\***



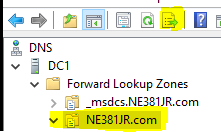
1. Now create a CNAME in the NE381XX.com forward lookup zone. Name the record **router** and link it to the FQDN of the gateway host record you just previously created. You will need to [browse] -> DC1 to accomplish this.  
   As shown below:

|  |
| --- |
| CNAME record linked to the FQDN gateway host record. |

1. From a DC1 command prompt type  
   **ping router.ne381XX.COM**

**What is the name and the address returned on the first line of the response? \* What does this tell you about the type of record you created? The name is gateway.NE381WB.com and the address is 192.168.1.1, the record is simply an alias for another record, in this case the gateway record.**

1. Verify on DC1 -> DNS that all CLIENT1, CLIENT2, DC1, and DC2 have host records.
2. Ensure the NE381XX.COM Zone folder is selected showing all the host records, then click on the Export List Button



Export all dns records to a file called ***NE381XX.COM\_DNS-Records*** to the Desktop

Part 3 More DNS settings and Replication

1. From the DNS Manager on DC1 right click on the DNS icon and select Connect To DNS Server



1. Select (\*) The following computer: and type **DC2** in the dialog box provided.

You should have just added DC2 into this DNS manager. You can now view and make changes on DC2.

|  |
| --- |
| Screenshot the new connection to DC2: |

1. Right Click on DC1 and go to properties
2. Click on the forwarders tab, then edit to add a forwarder to 4.2.2.2

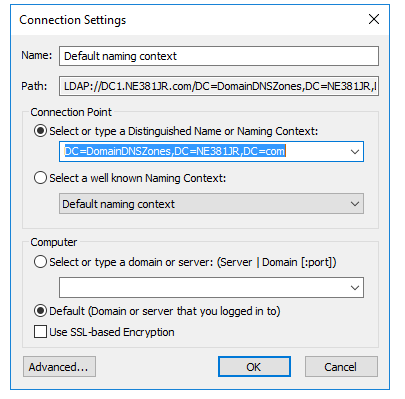
|  |
| --- |
| **Screenshot:** |

1. Exit the properties of DC1.
2. Open the properties of DC2. Click on the forwarders tab. Then entry you just made in DC1 does not exist here. This is because forwarders is a server specific setting and is not replicated. Close the Properties Dialog box
3. Expand the DC2 to the reverse lookup zones and verify two lookup zones; one for the 192 and another for10.  
   If you do not see this stop and ask for assistance.  
   These zones were replicated from DC1.  
   Zones are replicated, server settings are not.
4. Click on your DC2 -> Forward Lookup Zone NE381XX.com
5. Create a new A record called **joeyjoejoe** with an ip address of 192.168.5.6  
   Do you see the new record listed under the DC2 FLZ folder? **Yes**
6. Browse back to Forward Lookup Zones under DC1 and click the refresh icon.  
   Was the joeyjoejoe record replicated to the DC1 DNS server?

|  |
| --- |
| Screenshot the DC1 FLZ folder: |

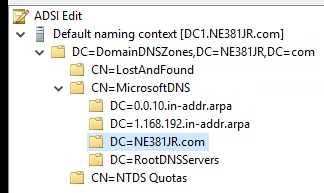
Zone information is replicated via Active Directory. This is because you have an AD replicated DNS setup. This allows for ease of management. Next you will observe the record being stored in AD.

1. From DC1 Server Manager -> Tools -> ADSI edit (Active Directory Services Interfaces Editor)
2. On the ADSI Edit Object Right Click and Select Connect To
3. Choose Select or Type a Distinguished Name or Context and type in DC=DomainDNSZones,DC=NE381XX,DC=com Then click OK



**Note that the domain name is not XX but whatever you named your domain.**

1. Now drill into CN=MicrosoftDNS then DC=NE381XX.com



1. In the right pane you should see all the dns records for your domain.

We are currently viewing all the dnsNode objects that are stored in AD. Sometimes when there is an issue with a zone or a record it may be necessary to remove the object from AD Database directly.

|  |
| --- |
| **Screenshot this listing of dnsNode objects:** |

1. Return to DC2 -DNS and locate the joeyjoejoe A record and delete it
2. This change should replicate to DC1 in a few minutes.
3. Back in the ADSI edit column you will notice that joeyjoejoe still exists in the AD file. AD will not automatically delete it.
4. Right Click on this record and find the Attribute dNS Tombstoned is set to True

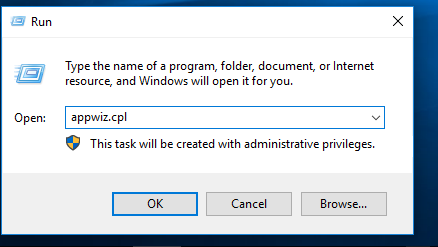


|  |
| --- |
| **Screenshot the entire record for upload to canvas\*** |

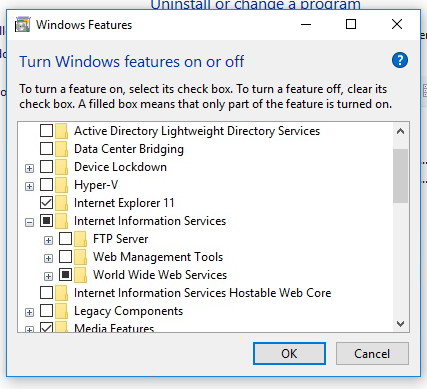
If the record is in this tombstoned state for 7 days it will be removed from the AD database. You can force removal in ADSIedit by right clicking on the object and deleting it. This is a great article on DNS record deletion.

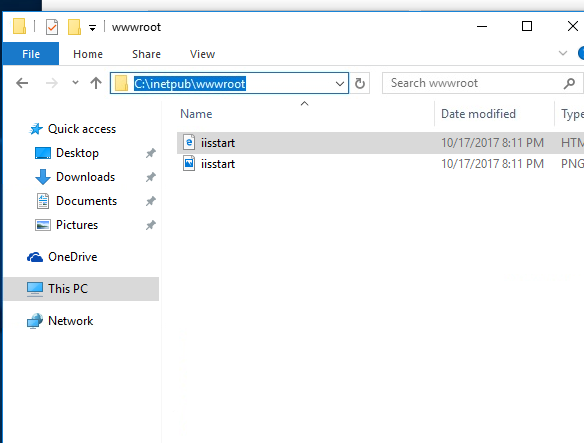
<https://blogs.technet.microsoft.com/networking/2011/08/17/tracking-dns-record-deletion/>

1. Login to **CLIENT1 as your Personal Domain Admin user account.**
2. Open a **run** prompt and type **appwiz.cpl**



1. Click **Turn Windows features on or off**
2. Expand **Internet Information Services** and check mark **World Wide Web Services**. It should look like this.



1. Click Ok
2. Once installation is complete navigate to **C:\inetpub\** and Add your personal admin **account** and **enable Full Control** permissions for the **wwwroot** folder.
3. Open the **iisstart.html** page with notepad and modify to Only contain the code below. Save when done.  
   
4. Open iisstart with notepad and edit it so it contains only this information.

<!DOCTYPE html>

<head>

<title>CNN</title>

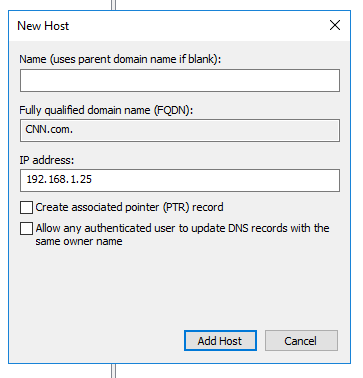
<body>

<h1>National Newsy Outlet!!</h1>

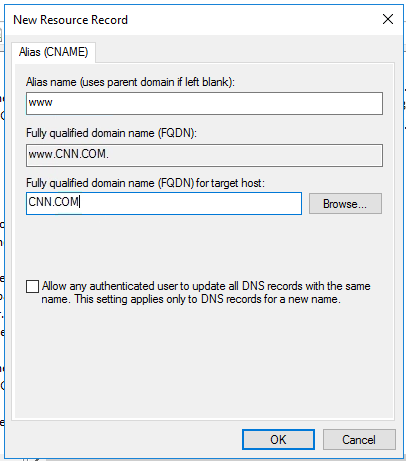
</body>

</html>

1. On DC1 Right-click DNS and **Create** a new Primary AD Integrated **Forward Lookup Zone** called **CNN.com**
2. Within this zone **create an A record** with a blank name and an ip address that is the same as your CLIENT1



1. Next create a CNAME of WWW that links back to the A record.

It will look something like this.  




1. Now on CLIENT2 open a command prompt and **ping** [www.cnn.com](http://www.cnn.com). Ensure it returns the ip address of your CLIENT1 ip.
2. On CLIENT2 Open a browser and navigate to [www.cnn.com](http://www.cnn.com)

If you did all the steps correctly, you should get a page that says Fake News.

|  |
| --- |
| **Screenshot this page for submission to canvas\*** |

You were able to successfully poison a DNS server and spoof a legitimate website.

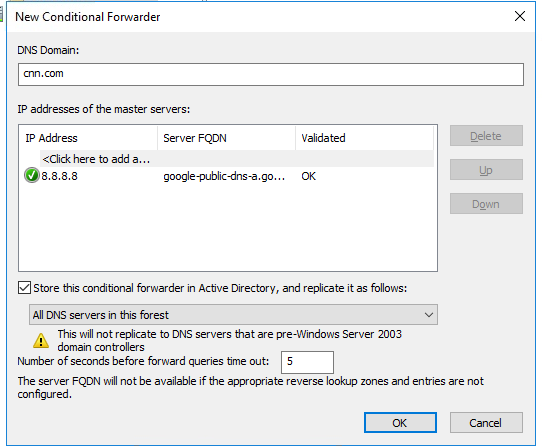
**\*\*This is why it is crucial that DNS is secured and its operations are handled by people who are familiar with DNS.**

1. From DC1 delete the CNN.com forward lookup zone.
2. Close CLIENT2 browser and Flush CLIENT2 DNS cache.
3. Reopen browser to CNN.COM

|  |
| --- |
| Screenshot CLIENT2 -> CNN.COM webpage: |

Part four DNS Conditional Forwarders and nslookup

1. DC1 -> In the DNS Management tool, Right-click [Conditional Forwarders] folder and Create a New Conditional Forwarder with the following properties.



1. On CLIENT2, open browser and logon to Canvas; download and install **Wireshark-win64-2.4.2.exe** from Canvas -> Week 3 folder.
2. Once install is complete. Run a capture on the **Ethernet0** interface by selecting Ethernet0 and then press the shark fin.
3. Now, while capture is in operation, Open an elevated command prompt on CLIENT2 and type **nslookup**
4. In the nslookup prompt type [www.foxnews.com](http://www.foxnews.com). **(do not forget the . at the end**
5. Open your wireshark and in the filter area put dns

 then click the arrow  on the right to apply the filter.

1. Locate the standard query A [www.foxnews.com](http://www.foxnews.com). And the Standard query response.

**What server responds to the client** **request?\***

**192.168.1.12 (DC1)**

1. On DC1 download and install wireshark.
2. From the same command prompt launch nslookup
3. Start a wireshark capture
4. At the nslookup type [www.cnn.com](http://www.cnn.com).
5. Locate the standard query and the standard query response for [www.cnn.com](http://www.cnn.com).

**What server responds to the query request\*?**

**8.8.8.8 (Google)**

Since we have a conditional forwarder in place for the cnn.com zone the dns server will always forward any requests bound for that domain to the server specified in the conditional forwarder.

**Why will the client always get a response from the domain controller.**

**In the client’s IP settings, the preferred DNS server is statically set to the DC1 IP address.**