# Overview

DNS name resolution is a core service of the Internet and a business network. It is primarily used to resolve DNS names to IP addresses that are used to identify devices in an IP network. In this guided practice you will explore the components and operation of the DNS service and protocol.

# Objectives

* Define or explain common terms and concepts related to DNS on Windows
  + Be able to use the nslookup command to test name resolution including the following:
    - Query for a specific type of resource record
    - Query a specific name server
    - Locate a root name server
    - Locate a top-level domain name server
    - Locate a second level domain name server
  + Be able to use the command line to view or clear the DNS cache on a DNS client
* Configure DNS on Windows server
  + Be able to install the DNS service role from the GUI and the command line

## Skills Reviewed

* Installing Software.
* Capturing network traffic with a protocol analyzer.
* Configuring DNS clients.
* Using nslookup to query a DNS server.
* Installing server roles on Windows Server.

## New Skills

* Configuring a caching-only DNS server.
* Testing a DNS server.
* Configuring and using PowerShell remoting in a Workgroup.

## References

* <https://activedirectorypro.com/use-nslookup-check-dns-records/>

# Initial Conditions

Your virtual machine should be in this state prior to beginning this guided practice:

* Guided Practice – **Configuring Hyper-V Networking** is complete.
* Connectivity exists between all servers in the virtual network.

# Final Conditions

At the end of this exercise:

* Caching only DNS server installed on Server-01
* All devices configured to use the DNS service on Server-01

# Instructions

## Create a Caching Only DNS Server in Windows

A caching-only DNS server is a DNS server that hosts no DNS zones. A caching-only name server only resolves queries for clients and caches the results. This is the default configuration for a DNS server in Windows when the DNS role is installed.

To create a caching-only DNS server on **Server-01**, perform the following:

1. Login to the **Server-01** virtual machine.
2. Open a **PowerShell** session or launch **Server Manager**.
3. Add the **DNS Server** role using PowerShell. The name of the role is **DNS**.

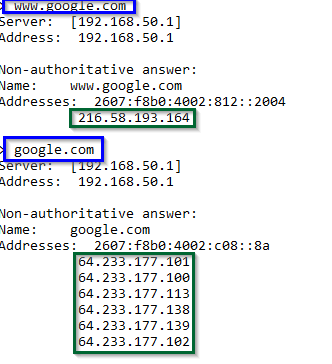
## Configuring DNS clients

1. On **Server-01**, configure the **Preferred DNS Server:** address on the LAN network adapter to use its IP address (10.1.1.1) as the preferred DNS server.

## Verifying DNS Client and DNS Server Configuration

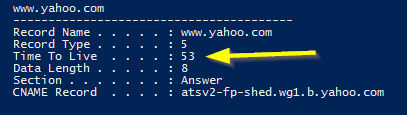
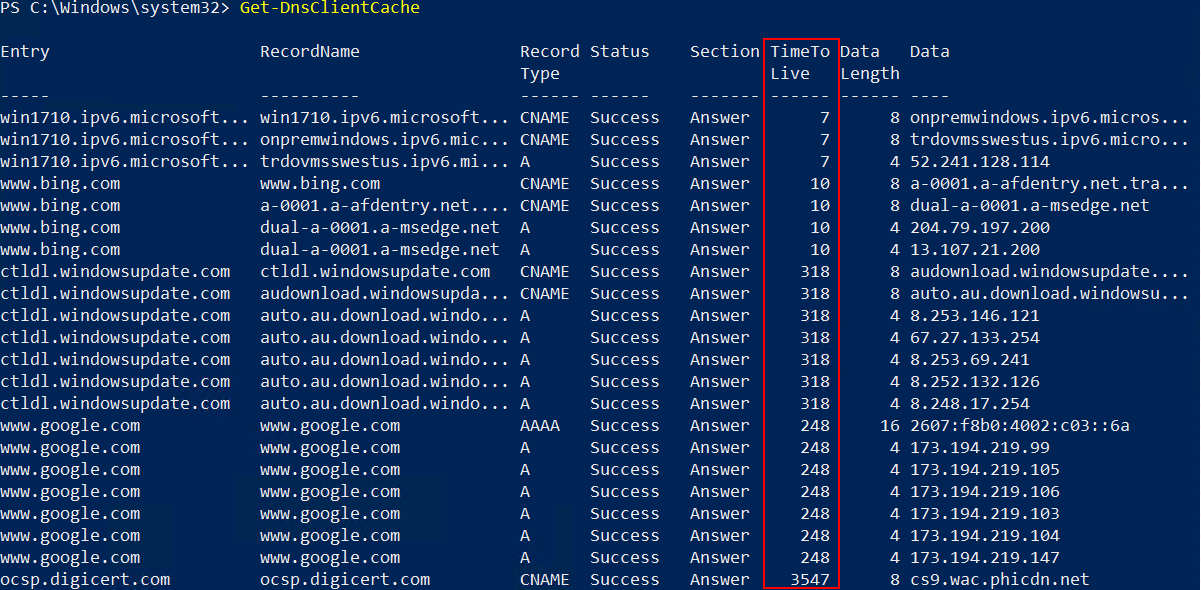
You can use the ***nslookup*** command to verify the configuration of both the server and the client. The ***nslookup*** command uses the configured preferred DNS server to query DNS and return a result. By using this command, you can test that the client is configured to use a DNS server and that the DNS server can resolve names.

1. Use the NSLOOKUP command to verify that the DNS server is functioning properly
   1. Execute **nslookup** from command prompt. The prompt is now the **nslookup** prompt **>.**
   2. Use **?** to view **nslookup** command syntax.
   3. Use the **server** command to set the default server to the IP address of **Server-01**. (At the > prompt, type **server 10.1.1.1**).
   4. At the **nslookup** prompt, enter the web site name of several sites and then enter their domain name. See the example below. The DNS server is resolving recursive queries for host & domain names outside of Hyper-V. Notice that the IP address returned for the **www.google.com** differs from any of the addresses returned for **google.com**.



1. Configure network adapter on **Server-02** to use the IP address of **Server-01 (10.1.1.1)** as the **Preferred DNS server**.

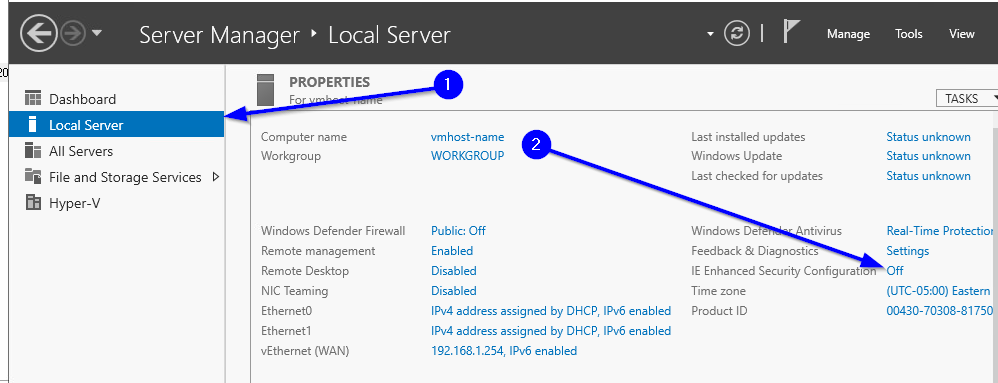
Set-DnsClientServerAddress -InterfaceAlias LAN -ServerAddress 10.1.1.1

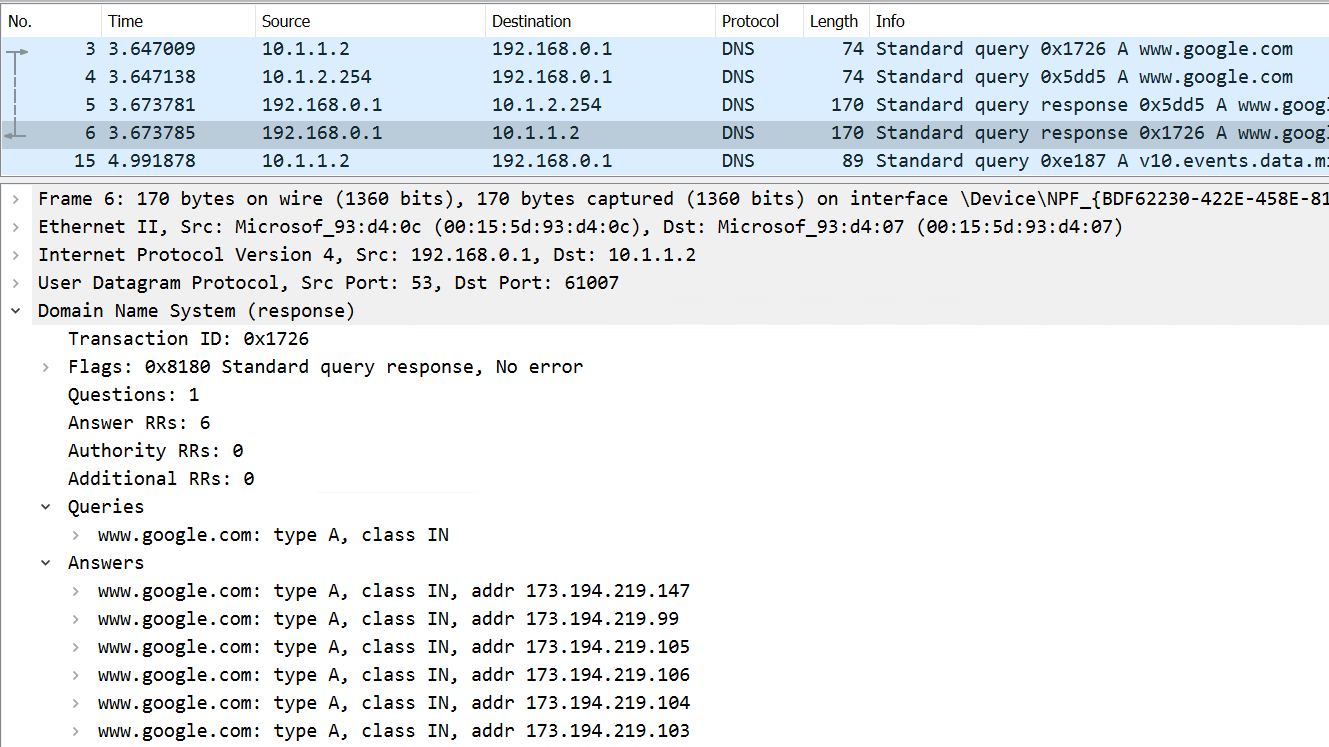
1. Use the NSLOOKUP command to verify that the DNS server is functioning properly.
   1. Execute **nslookup** from command prompt.
   2. Use the **server** command to set the default server to the IP address of **Server-01**.
   3. Use **nslookup** to verify that the DNS client can query the address of Internet hosts **att.com** and **ecpi.edu**.
   4. Close **nslookup** by issuing the **exit** command.
   5. Configure **network** **adapters** for the **Client-01** and **Client-02** to use the Preferred **DNS** Server: **10.1.1.1** (Remember you can do this using Powershell in **Server-01.**)
2. Test the **DNS** **client** configuration.
   1. Use the **Resolve-DnsName** cmdlet to determine the IP address of **www.yahoo.com**.
   2. `Use the **ipconfig /displaydns** or the **Get-DNSClientCache** command to view the DNS cache. Note the Time to live for some of the entries.
   3. Wait a few seconds and issue the **ipconfig /displaydns** command to view the DNS cache. How did the **Time to Live** (TTL) values change? Wait a minute and use **ipconfig /displaydns** command to view the DNS cache. Yes, the cache is empty because the TTL values were less than 60 seconds, thus they were removed from cache.

## Capture DNS query with Wireshark

It is often necessary when studying or troubleshooting DNS to use a protocol analyzer. This allows you to see the actual packets traveling back and forth between the DNS client and server. In this section, you will use Wireshark to view this traffic.

1. Login to the **Server-01** virtual machine.
2. Disable **IE Enhanced Security Configuration**
   1. In **Server Manager** click **Local Server** and then set **IE Enhanced Security Configuration** to **Off**. This change is needed so that the **Local Administrator** can download files.



1. Download and install the current stable release of **Wireshark** from <https://www.wireshark.org/#download>.
   1. Open Wireshark and start a capture and capture DNS packets. Ping [www.google.com](http://www.google.com). Find the packet with the DNS response that has the IP address of [www.google.com](http://www.google.com). Capture a snippet of the capture that shows the frame with the IP address of [www.google.com](http://www.google.com) and the Destination address of **SERVER-01 LAN** network adapter. Save the snippet as **DNS\_Google.com\_*studentID*.png**

# Submission Requirements

1. **Download** the **grading** **script** from the assignment page to the **C:\Scripts** folder.
2. Check your lab by running the following command:

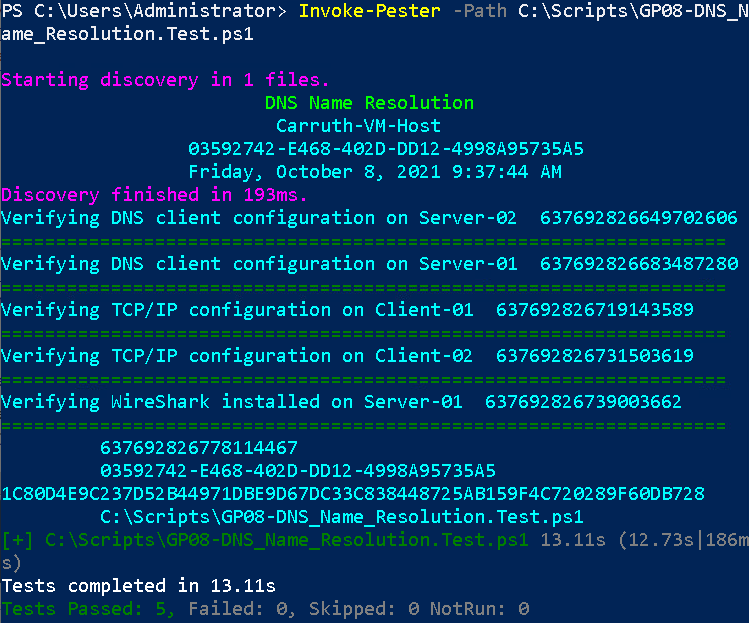
Invoke-Pester -Path C:\Scripts\GP08-DNS\_Name\_ Resolution.test.ps1

**Note**: You will see a security warning when running the script. Enter **R** to run the script.

If you want to see more detail, add **-Output Detailed** to the command. This may assist you with troubleshooting

Invoke-Pester -Path C:\Scripts\GP08-DNS\_Name\_ Resolution.test.ps1 -Output Detailed

1. You should not see any red in the output. Red in the PowerShell way of telling you that an error condition exists. Most of the time, the output will tell you what is wrong. If it is not obvious, contact your teacher and ask for assistance. You will be learning PowerShell during this term. **Correct** any **errors** you may have and run the script until all the output has no red. You should see the output like the images below.



1. Capture a snippet that shows the PowerShell Command and all its output. If you must use more than one snippet to capture the output, you must have at least **one line of overlap** in the snippets. The text in the snippets **must be legible** when pasted into the Word document. Paste the snippet(s) into a **new** **Word** **document**
2. **Paste** the **DNS\_Google.com\_studentID.png** into the **Word** **document.**
3. **Fill** **in** the **information** in the following table. Copy the following table into the **Word** **document** and fill in the information about all the **new** commands used in this lab (the example provided is not a new command and should be deleted):

|  |  |  |
| --- | --- | --- |
| PowerShell Commands | | |
| Command | Example | Description |
| *Get-Childitem* | *Get-Childitem -Path C:\* | *Displays the files in the C:\ directory* |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. **Upload** the **Word** **document** in the submission area of the assignment.