CSE 6032 Computer Networks
2021/22 Spring Term

Project: 2 – Part 2
Topic: Deploying Primary DNS Server
Date: 13.03.2022 – 22.03.2022

Objectives:

- to install a **primary** authoritative DNS Server
- to configure DNS Zones with **Windows Server2012**
- to analyze DNS service and protocol with **Wireshark**

Reference

- **Managing W'2012 DNS server** (https://krypted.com/windows-server/managing-dns-in-windows-server-2012/)
- **IANA DNS Parameters** https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml

Section A. Project Definition and Testbed Deployment

A.1 Project Scope

The project aims at deploying **DNS server** "mydns**"** as the primary **Authoritative DNS server** for the "**cen.net.**" domain. The "**cen**" domain is private given that:

- ✓ the FQDN "**cen.net.**" has not been registered by a **TLD** registrar in charge of the "**net.**" domain**;** and
- ✓ the Host-only Network subnet (LAN) is assigned the **private IPv4 @** block "**172.16.3.0 /24**", valid only within the limits of this subnet**.**

Nevertheless, Guests connected to the Host-only Network and configured to use "mydns**"** **DNS service** may resolve the names and addresses defined the private domain seamlessly**.**

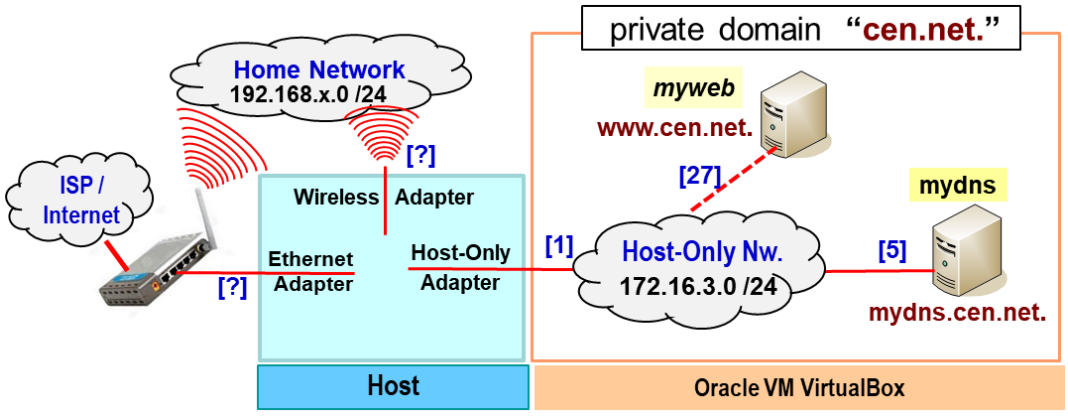
In coming projects, you will configure a gateway (border router) interconnecting Home Network and the virtual network. This will allow Guests to access real subnets through gateway's **NAT** (*Network Address Translation*) service and make them accessible from external networks via its Port Forwarding service.

A.2 Testbed Topology

Testbed depicted here has the same topology as in previous projects. Functionally, **VirtualBox DHCP service** is disabled to avoid unnecessary frame traffic and Guests' network settings will be configured manually.

On the drawing

- ✓ **yellow** tags designate "**computer names"** used by the **OS**;
- ✓ **brown labels** are systems' **FQDN** and will be registered at the **Authoritative DNS server**.
- ✓ **dashed** network connection for **myweb** system implies that the Guest **VM** is part of the private domain name space, but not deployed yet, Nevertheless, its DNS RRs can be registered and resolved by "mydns**"**.



A.3 Configuring Host's Host-only Network Adapter and VirtualBox DHCP Service

i) Verify that Host's Host-Only network adapter is assigned the CIDR IPv.4 @ **"172.16.3.1 /24"** and configured, as specified in Project 1 - Part1 section **C.4**.

ii) Disable **VirtualBox DHCP** service from "**DHCP Server**" configuration window (in Project 1 - Part 1 section **C.5**) by **unchecking** the "Enable Server" box.

iii) Once the above configurations are completed:

- ✓ stop **VirtualBox**;
- ✓ restart the Host (W"10) to reinitialize it's routing tables; and verify the correctness of Host's network settings using the "ipconfig /all" command.

Section B. Importing and Configuring DNS Server

B.1 Characteristics of the DNS Appliance

DNS server is a professional appliance running on a **64-bit** VM configured with **1 CPU**, **1Gb** RAM and **15 GBytes** hard disk operating under Windows Server2012 R2 licensed to IKU.

DNS server has been exported as the "**WS2012-Ref.ova**" appliance, after following the customizations.

- ✓ **DNS** and **DHCP** server applications have been **installed** (in Microsoft terms their **administrative roles** have been defined); **DNS service** is not configured, but the **DHCP service** has been configured for the test scope "**10.0.2.0**".
- ✓ **Automatic OS updates** are disabled (Control Panel -> Windows Updates, use "*Change Settings*" option to set 'never check for updates').
- ✓ **Windows Firewall** is turned off for Home and Public Networks (Control Panel -> Windows Firewall menu, use '*Turn Windows Firewall On or Off*' option).
  Note that, you have **to check these settings** each time you **connect** the Guest to a new network and/or add a new network adapter.
- ✓ **Power option** that turns the **display** and the **disk** off are set to **stay active** for several hours.
  (Control Panel -> Power options, select "*My Custom Plans 1*" then use 'When to turn off the display" option).
- ✓ **Wireshark** analyzer has been installed.
- ✓ **Network adapter 1** is configured to '**Obtain an IP address automatically**' from a DHCP server.

B.2 Downloading Guest Appliance

Download the appliance **"**WS2012-Ref.ova**"** from University's **ftp server** or use the alternative **google drive**, as specified in the **Project Definition** section of **Project-2 Part-1,** if you have not done it yet**.**

B.3 Importing the Guest and Connecting it to Host-only Network

Perform the following steps to import and configure the Guest.

i) Start **VirtualBox Manager** and set the "**Default Machine Folder**" to e.g. "**C:\VMs**" ("**File->Preferences**" path).

ii) Import "WS2012-Ref.ova" appliance after changing its name to "**MyDNS**".

iii) Once imported, review MyDNS settings by clicking on the "**Settings**" icon, and make sure that there are no VirtualBox configuration "**Warnings**".

vi) Select **"Adapter 1**" tab, and verify that:

- ✓ "Enable Network Adapter" box is checked;
- ✓ adapter is "Attached to" to the "Host-only Adapter" (if not correct it using the pull-down menu);
- ✓ **"**Promiscuous Mode**"** under the **"Advanced"** submenu is set to "Allow All" option.
- ✓ "Cable Connected" box is checked.

B.4 Customizing the Guest OS

Perform following steps to install **VirtualBox Guest Additions** on the **Guest OS** for seamless Host/Guest integration.

i) Power on MyDNS and log in as '**Administrator'** using the password "**Qwer1234**".

Note that since the "**ctrl-alt-del**" key combination is dedicated to the Host`, you cannot use it to log on to VMs. **VirtualBox** defines the "**right ctrl + del**" key combination as the alternative setting.

ii) Insert **Guest Additions CD image**, using VirtualBox Menu's **Devices** Tab. (may take a few seconds).

iii) Open **File Browser** and select **CD** drive (**D:**); double click on "VBoxWindowsAdditions" to run it.

iv) Once the update ends DO NOT Reboot MyDNS, just shut it down using the Power Off icon on the top right.

v) Remove "VBoxGuestAdditins.iso" using the procedures outlined in **Section D.5/i** of the Project 1 - Part 1.

B.5 Configuring MyDNS Network adapter

Configure MyDNS network adapter (the Ethernet connection) manually, using the procedures outlined here after.

i) Power on MyDNS and log in as '**Administrator'** using the password "**Qwer1234**".

ii) Open "**Network and Sharing Center"** and select the Ethernet connection.

iii) Use the procedures **(iv)** through **(vii)** outlined in **section C.4** of the **Project 1 – Part 1** *-that you have used to configure the Host-Only Network adapter of the Host manually-* and assign the following values:

- ✓ **CIDR IPv.4 @**: **172.16.3.5 /24**
- ✓ **Default gateway**: the IP@ of the Host connection to the Host-only Network.
- ✓ **Preferred DNS Server**: **127.0.0.1** the IP@ of the virtual **loop-back** network interface**.**

  Loop-back network "127.0.0.0 /8" is a virtual network crated by the TCP/IP protocol stack in each OS. Frames sent to this internal network are never passed to any network interface controller or hardware. **Link Layer** delivers them all to the virtual loop-back network adapter, to the "localhost" connection, that is assigned the CIDR IPv4@ "127.0.0.**1** /8". Refer to lecture notes to understand the rational of this setting.

iv) **Note that** this configuration may create a new network connection definition for this adapter e.g. "Network 3". Consequently, appliance original firewall settings documented **in Section B.1** may have been altered.

Open the Windows Firewall menu through Control Panel and use 'Turn Windows Firewall On or Off" menu to turn off **Windows Firewall** for Home and Public Networks.

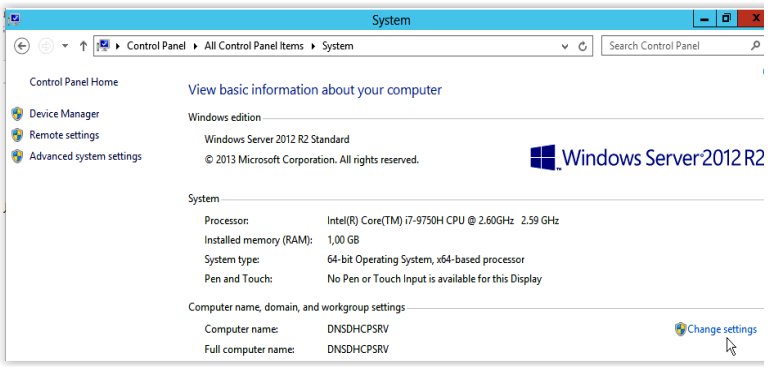
B.6 Configuring MyDNS Name and Primary DNS Suffix

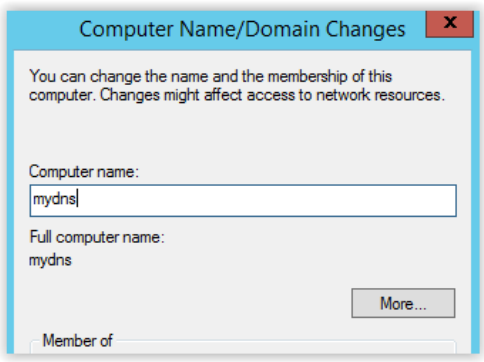
i) Open 'System' menu through Control Panel (left screen shut here after); and click on "Change Settings**"** link located at the right corner (marked by the mouse pointer).

ii) On "System Properties**"** window click on the "Change**"** button to open "Computer Name/Domain Changes**"** window (right screen shut):

- ✓ enter the system label "**mydns**" in the "Computer Name**"** field;
- ✓ click on the "**More"** button and enter your **Primary DNS Suffix** "**cen.net.**" (do not omit the dot);

  → Note that each time you use a PQDN in a tool **this suffix** is **appended** to form its **FQDN**.
- ✓ accept all the changes by pressing "**OK**"s; and restart the system.





iii) **Confirm** your settings with "**ipconfig /all**" command (take its screen shut and paste it as the answer #1 of the project report) and by pinging MyDNS from the Host and vice-et-versa (if your Host's firewall settings allow it)!!

iv) Note that the "**ipconfig /all**" command listed at the end the Tunnel adapter "**Microsoft ISATAP Adapter**" that can be used to connect this server to IPv6 networks. As this support will not be used and will create additional network traffic that interferes with **Wireshark** captures, you can disable it each time you power on the server.

→ Open command line window with **administrative rights** or Windows PowerShell, and run the command:

netsh interface teredo set state disabled

Section C. Configuring DNS Service

An authoritative DNS server such MyDNS as may be configured:

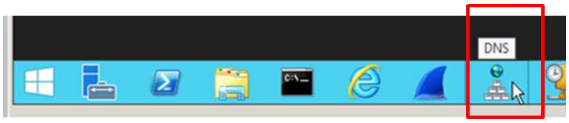
- ✓ to manage the **entire** "cen.net." domain as a single administrative zone, or
- ✓ to partition the domain into several zones and delegate their **responsibility** to other DNS servers.

Within the scope of this project, you will deploy only one **authoritative** DNS server for the "**cen.net.**" domain; and configure it as a **single** administrative zone.

Note that, in practice even if a domain is organized as a single administrative zone, several **secondary authoritative** DNS servers are deployed for reliability and performance. You are invited to refer to lecture notes for further explanation on **primary** and **secondary authoritative** DNS servers and how they synchronize to match their contents after updates.

C.1 Activating DNS Service

The DNS service is already activated on MyDNS (check the first reference for how?), you may start configuring it using the **DNS Manager** that is run by clicking its icon as shown on the right.



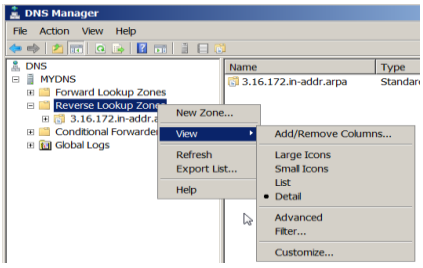
C.2 Exploring Default DNS Service Configurations

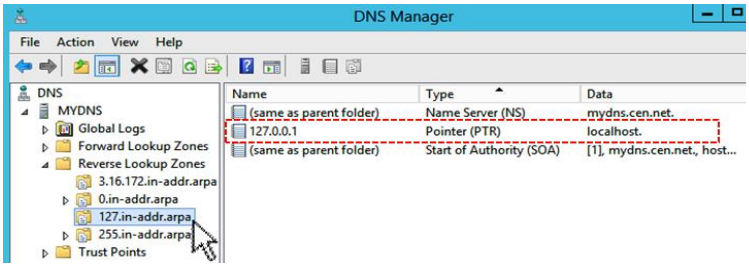
DNS service installation generates several default configuration options & parameters. Out of them we will explore only two: the definition of the reverse loop-back zone and the **list** of root servers.

i) Displaying Hidden Reverse Zones

DNS service installation has generated **three** hidden Reverse Lookup Zones. Display them as fallows.

- ✓ Start the **DNS Manager;** select & expand MYDNS on the left pane (left screen shut here after).
- ✓ Select and right click Reverse Lookup Zones line to open the pull-down menu (*left screen shut*).
- ✓ Select the "**View**" entry and check the "**Advanced**" option.
- ✓ Select the 127.in-addr.arpa zone as shown on the right screen shut here after, and identify on the right pane the definition that maps the **FQDN** "localhost." to the **IP@** "127.0.0.1" with a **PTR** type of RR record.





ii) Testing DNS Server Connection and Reverse Name Resolution

Perform the following to test the "**Preferred DNS Configuration**" defined in **Section B.5/iii** and to observe the reverse name resolution process.

- ✓ Start **Wireshark**; reset its "**Address Resolution**" options using Project-1 Part-2 **Section B.3**.
- ✓ Start capturing frames over the "Adapter for Loopback traffic capture" (why?).
- ✓ Run "nslookup**".**

- ✓ **Resolve** the reverse IP@ of the loop back network adapter using the commands:
  - **set type=ptr**
  - **1.0.0.127.in-addr.arpa.**

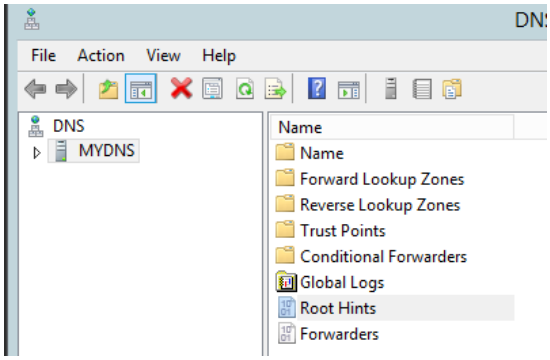
  You should have the "localhost" label displayed.
- ✓ Stop **Wireshark**; analyze captured **L2** frames and identify the frames:
  - nslookup used to display the name of the "**Default Server**"
  - used to resolve the reverse query **1.0.0.127.in-addr.arpa.**

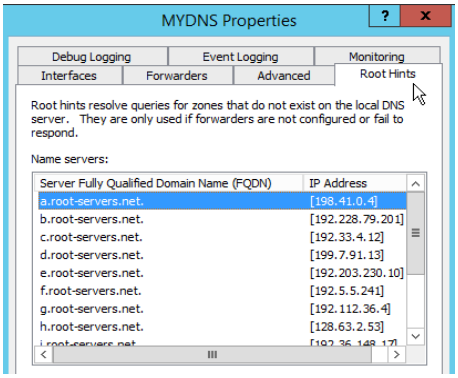
  save the capture to answer question #2 of the report.

iii) Displaying the List of Root Servers

Your DNS service is configured to resolve the names that are defined within the **"**cen.net." domain. The server will attempt to resolve any query such as **"**ieee.org.**",** that is not part of your zone of authority, through its authoritative server. Thus, it should have access to the list of root servers.
Display the list of predefined root servers as follows.

- ✓ Start the **DNS Manager;** select MYDNS icon on the left pane (left screen shut here after).
- ✓ Double click "**Root Hints**" line on the right pane to open the MYDNS Properties window (*right screen shut*).





iv) Testing the use of List of Root Servers

To test how the DNS service uses the root servers to resolve the FQDNs that are not defined in the **"**cen.net." domain perform the following.

- ✓ Start **Wireshark**; reset its "**Address Resolution**" options.
- ✓ Start capturing frames over "Host-only Network" instead of the "Adapter for Loopback" (why?).
- ✓ Run "nslookup**"** and resolve **"**ieee.org.**"**
- ✓ Stop **Wireshark** after DNS service attempted to contact at least **4 root servers.**
- ✓ Analyze captured L2 frames and identify:
  - the frames sent to root servers defined in the "**Root Hints**"
  - Why none of these queries got an answer?

  save the capture to answer question #2 of the report.

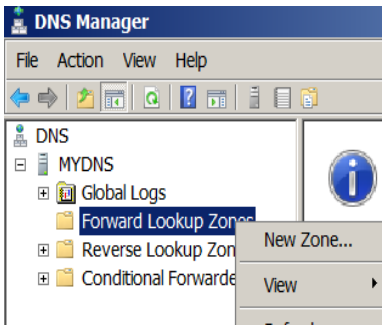
C.3 Creating Primary Forward Lookup Zone for the "cen.net." Domain

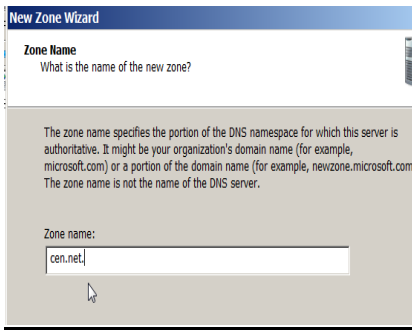
In DNS terminology, "Forward Lookup Zone" refers to the set of **RR**s (Resource Records) that map FQDNs to their IP @**.** Conversely "Reverse Lookup Zone" refers to **RR**s that define IP@ → FQDN mappings.

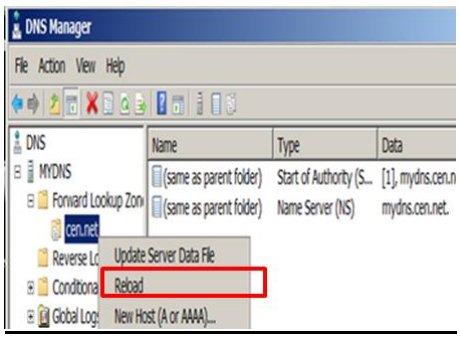
i) Define the **primary** Forward Lookup zone of the "**cen.net.**" domain using the procedures outlined here after.

- ✓ Start the **DNS Manager;** select & expand MYDNS entry on the left pane (left screen shut here after).
- ✓ Select and right click **Forward Lookup Zones** line; select the **New Zone** definition.
- ✓ Proceed with the **New Zone Wizard** and choose the **Primary Zone** alternative; click-on **Next** button.

- ✓ Enter the zone name "**cen.net.**" (do not omit final dot! As shown on the middle screen shut).
- ✓ Accept the default file name "cen.net.dns" where zone data will be stored.
- ✓ Select '**Do not allow dynamic updates'** option; then '**Finish'** configuration process.
- ✓ Select MYDNS icon on the left pane; update the server by selecting from the menu "**Action -> Update Server Data Files**".
- ✓ On the left pane expand **Forward Lookup Zones** entry; select the "cen.net." zone (right screen shut below); and update DNS table loaded in memory by "**Action -> Reload**".





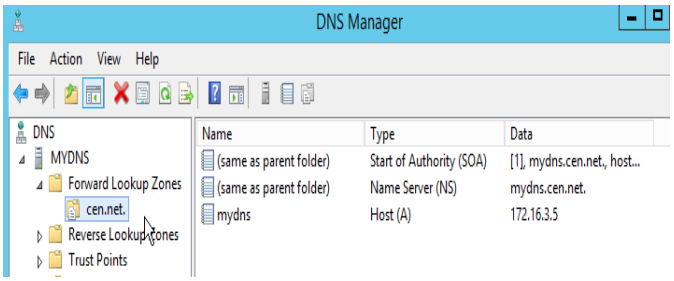


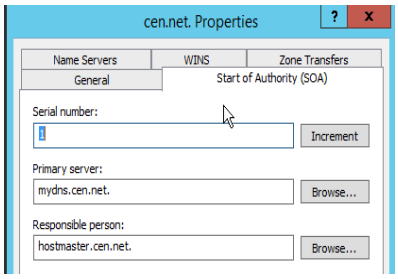
ii) Verify that "cen.net." zone contains the following **3 RR**s (left screen shut here after).

- ✓ **Start of Authority** (SOA) defining the attribute to be returned with the replies **TTL**, refresh interval etc.
- ✓ **Name Server** (NS) the FQDN "mydns.cen.net.", and
- ✓ **Host** (A) the IP Address of the name server "172.16.3.5".

iii) Click on the SOA RR on the right pane to open "cen.net. Properties" window; and identify:

- ✓ "**serial number**" keeping track of **RR**s version that should be incremented at each update (why?);
- ✓ time attributes associated with **RR**s etc.
- ✓ examine **all** the other Tabs (General, Name Servers etc.).





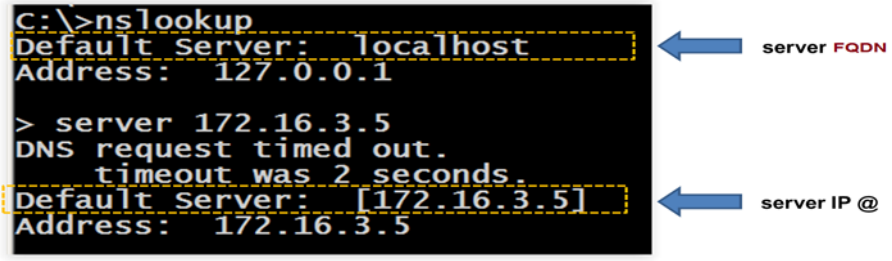
iv) Click on the **Name Server** '**NS**' **RR** on the right pane and confirm its FQDN.

v) Examine the 'Host (**A**)' **RR** definition and confirm FQDN ↔ IP@ matching.

C.4 Testing Primary Forward Lookup Zone for the "cen.net." Domain

Perform the following procedures on MyDNS to test its OS and DNS service settings.

i) Run "**nslookup"** and change default DNS server by entering the command "**server 172.16.3.5"**; the output should be similar to the one displayed here after, if not revisit **C.3/ii**.



- ✓ What caused the time out after you have entered the "**server 172.16.3.5**" command?
- ✓ Why nslookup labeled the "**Default Server**" by its **IP@**, rather than its **FQDN**?

ii) Resolve the PQDN "**mydns**"; the output should be like the one displayed here after, if not revisit C.3/ii.

```
> mydns
Server:  [172.16.3.5]
Address:  172.16.3.5

Name:    mydns.cen.net
Address:  172.16.3.5
```

Try to explain how nslookup managed to resolve PQDN and displayed correct FQDN and IP @ of the system? Hint. You may use the information displayed by the "**ipconfig /all**" command.

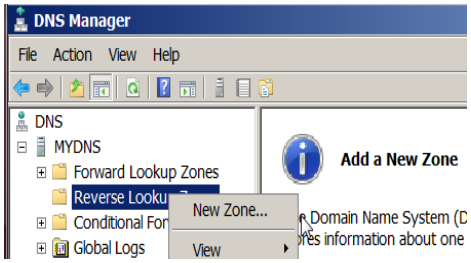
C.5 Creating Primary Reverse Lookup Zone for the "cen.net." Domain

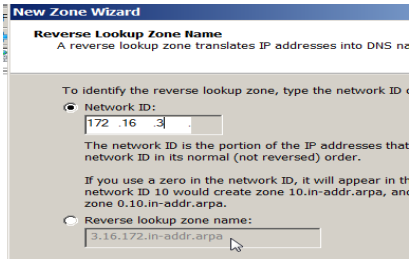
In **DNS server** terminology "Reverse Lookup Zone" refers to the collection of RRs that map zone entities' reverse IP @ to their FQDN (represented in DNS databases by the **PTR** (pointer) **RR** type).

i) Define the **primary Reverse Lookup zone** for the "cen.net." domain using the procedures outlined here after.

- ✓ Start the **DNS Manager;** select & expand MYDNS entry on the left pane (left screen shut here after).
- ✓ Select and right click **Reverse Lookup Zones**, select "**New Zone"** and click **Next**.
- ✓ Choose **Primary Zone** radio button on the **New Zone Wizard** menu, click **Next**.
- ✓ Select **IPv4 Reverse Lookup Zone** option, press **Next**.
- ✓ Define **Network Id** of the zone "**172.16.3.0 /24**" as"**172.16.3**" (**right screen** shut below), click **Next**.

  Note that
  - + data entry screen allowed you to enter only the **Network Id** information!
  - + the **Reverse lookup zone name** "3.16. 172.in-addr.arpa" is automatically generated.

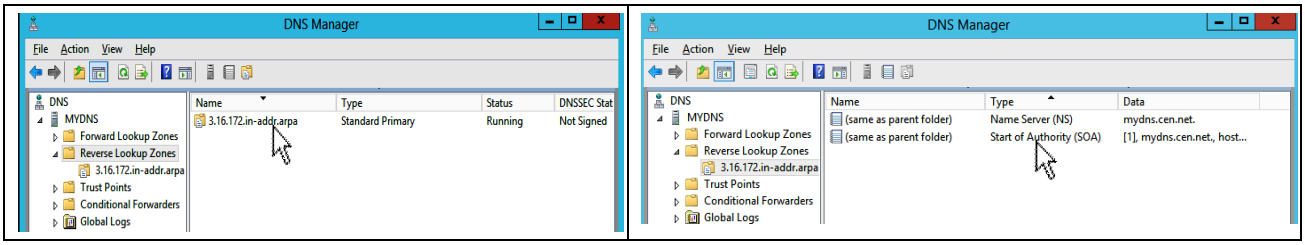




- ✓ Accept the creation of the **new reverse zone**, as well as its **default file addresses**, and then click **NEXT.**
- ✓ Select "**Do not allow dynamic updates**" option; click **NEXT** and finalize the installation process.
- ✓ Select MYDNS icon; update the server by selecting from the menu "**Action -> Update Server Data Files**".

ii) To verify **Reverse Lookup Zone** definitions perform the following.

- ✓ Select "Reverse Lookup Zones" on the left pane.
- ✓ On the right pane double click Reverse Lookup Zone you have just created (left screen shut here after).
- ✓ Open the **SOA** record (right screen shut) and check the parameters defined for the **Reverse Lookup Zone**; what is TTL for this RR?

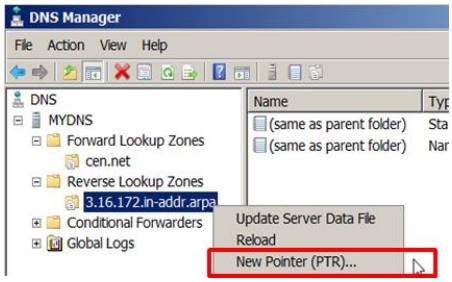


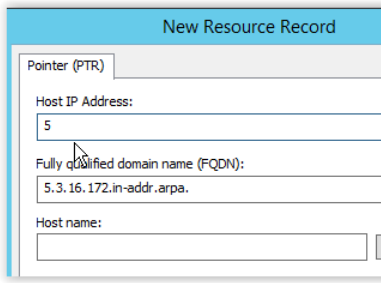
C.6 Defining and Testing Reverse IP@ for "mydns.cen.net."

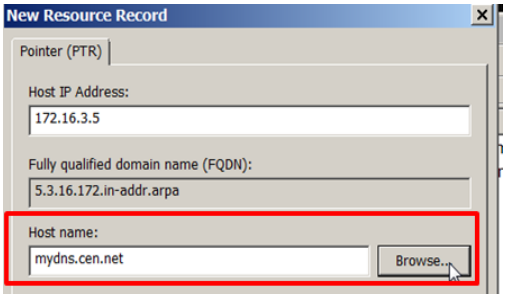
i) Define the reverse IP@ for "**mydns.cen.net.**" using the procedures outlined here after.

- ✓ Start the **DNS Manager;** select & expand MYDNS entry on the left panel then **Reverse Lookup Zones**.
- ✓ right click the "3.16.172.in-addr.arpa" zone, (left screen shut here after), and select the **New Pointer (**PTR**)**.
- ✓ Enter Host-Id (5) of the server (middle screen shut below).
- ✓ Fill the "**Host name**" field by browsing server's FQDN from list displayed in the **forward zone.**

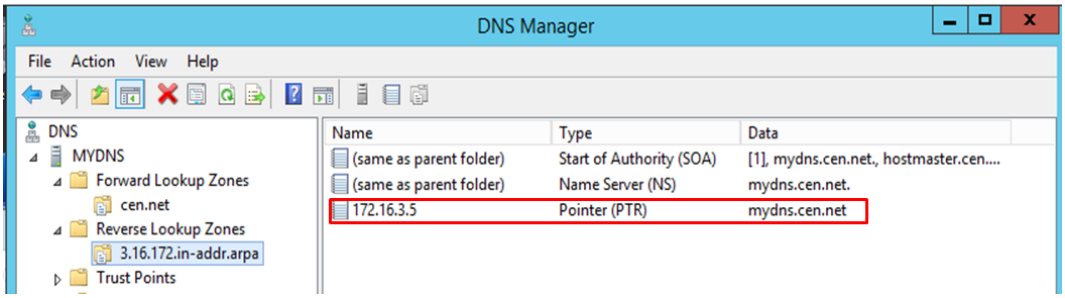
  Note that the "**Host Name**" field should display FQDN "mydns.cen.net." as shown on the right screen shut here after if all your definitions are correct (if not revisit them).







- ✓ Update the server by selecting from the menu "**Action -> Update Server Data File**".
- ✓ Verify that your reverse IP@ record for "mydns.cen.net." looks like the one displayed here after.



i) To test your reverse zone configurations, perform the procedures here after.

- ✓ Run **nslookup** and change the DNS server to MyDNS by entering just its PQDN "**server mydns**" the Server; name of the Default Server should be displayed as shown here after.

```
C:\Users\Administrator>nslookup
Default Server:  localhost
Address:  127.0.0.1

> server mydns
Default Server:  mydns.cen.net
Address:  172.16.3.5
```

ii) Perform a **reverse domain query** to retrieve the FQDN corresponding to the IP@ **172.16.3.5** to obtain an output that looks like the following.

```
> set type=ptr
> 5.3.16.172.in-addr.arpa.
Server:  mydns.cen.net
Address:  172.16.3.5

5.3.16.172.in-addr.arpa name = mydns.cen.net
>
```

Section D. Adding New Definitions to the "cen.net." Domain

D.1 Defining RRs of a New System

MyDNS has been configured as **primary** authoritative **DNS sever** of the "cen.net." domain. After this step, defining new systems part of this domain (adding their forward & reverse zone RRs) can be performed with a single transaction.

Use the procedures outlined here after to add DNS RRs for the web server "www.cen.net.**"**.

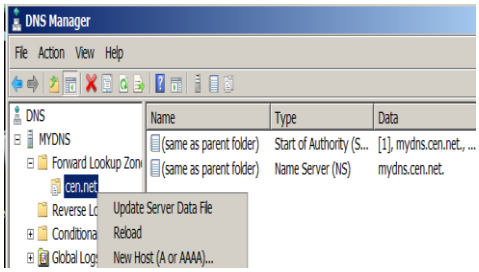
i) Start **DNS Manager**, expand **Forward Lookup Zone.**

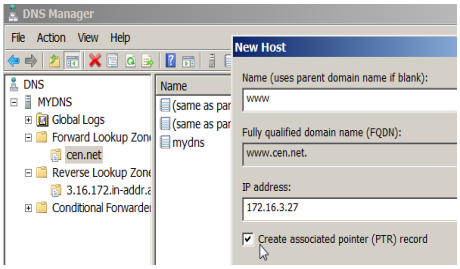
ii) Right click on the "cen.net." **zone** (left screen shut here after), select the **"New Host** (A or AAA)" option.

iii) Fill the "**New Host**" window's
- ✓ "**Name**" field with **www**; and
- ✓ "**IP address**" field with **172.16.3.27** (right screen shut below).

iv) Check the box "**Create associated pointer (PTR) record**" to generate reverse zone RR at the same time.

v) Press the "**Add Host**" bouton.





vi) Expand "cen.net." **zone** and verify that the **A** type **RR** has been properly created for the label "www".

vii) Expand the reverse zone "**3.16.172.in-addr.arpa**." and verify that www's **PTR** is properly created.

D.2 Testing the RRs of "www.cen.net."

i) On MyDNS start **nslookup**
- ✓ resolve the **PQND "www";**
- ✓ resolve the reverse IP@ of **"www"** (**"27.3.16.172.in-addr.arpa.");**
- ✓ verify that the queries are correctly resolved; if not review all the settings you have performed in Section D.

ii) Take the screen shut of the command window containing both queries and save it as "d2.png" or "d2.jpg".

D.3 Testing DNS Server From the Host

i) Clear the ARP tables on the Host and on the MyDNS with "**arp -d ***" commands; and check them with "**arp -a**".

ii) Run **Wireshark** on the Host or on the MyDNS if the Host does not capture the Host-Only Network traffic.

iii) Uncheck **Wireshark**'s the **Name Resolution** options; start capturing the Host-Only Network traffic.

iv) Run **nslookup** on the Host; enter the "set type= A" directive and resolve the PQND "www**"**
Was the PQDN resolved? Did Wireshark capture any related frame?

v) Change the DNS server to "mydns**"** with the "server 172.16.3.5**"** directive.

vi) Resolve the FQND "www.cen.net.**"**.
The FQDN must have been resolved and **Wireshark** captured related frames. If not change capture system.

vii) Resolve the FQND "www.cen.net." and its reverse IP@.

viii) Take the screen shut covering the steps (v), (vi) and (vii) and save it as "dns.png" or "dns.jpg"

ix) Stop capturing; store it as the "dns.pcapng" file.

x) Identify out and mark the ARP and DNS L2 frames that involved in resolving "www.cen.net." and the reverse IP@ in steps vi and vii**;** then prepare the **Packet Summary Line Report** and store it in the "dns.txt" file.

Section E. Preparing & Submitting Project Report

E.1 Preparing the System Identity Certificate

On the **Host** open the command line interface with **administrative** rights and perform the following:

- ✓ store the output of your "**ipconfig /all**" command in a **text file** labelled with your **studentid;**

  ipconfig /all > c:\....\180000xxxx.txt

- ✓ change your current directory to **"\Program Files\Oracle\VirtualBox"**;
- ✓ run the command **VBoxManage showvminfo MyDNS**
  note that the name of the VM should be written exactly as it is displayed by the VirtualBox Manager!!!
- ✓ If you are successful in displaying **W7-1** information append it to the previous **text file** with:

  VBoxManage showvminfo MyDNS >> c:\.....\180000xxxx.txt

The project will not be graded if the System Identity Certificate is not submitted

E.2 Preparing Project Report

Use the information you gathered to prepare the project report "**Prj2-Part2- Report.docx**" stored at CATS course portal under the Resources/Project Appendices folder.

E.3 Report Submission

Compress the files listed here after using the **Compress Project Reports** stored under **Resources/How to?** Folder.

- ✓ **Prj2-Part2- Report.docx**
- ✓ **System Identity Certificate** the **180000xxxx.txt** file
- ✓ "**dns.pcapng**" and "**dns.txt**".

Store compressed report in the **Prj2-Part2** folder located under **Assignments** heading at the course portal CATS **CSE6032-SectionX**; where "X" stands for (1.2.3.4), the laboratory session group you are registered in.

Collaboration Rules: What is Allowed What is NOT

Collaboration is a great way to learn. Students are encouraged to **discuss** project concepts and confer on **implementation** procedures with their peers. The key is to **use collaboration** as a way **to enhance learning**, **not** as a way of sharing answers without understanding

To avoid **plagiarism** all prose and code that you write for projects must be your own original work. Any other source you use must clearly identify and accurately cited.

Submitted work should be exclusively yours; **copying** or **getting help** from a third party is prohibited. Your submissions should be kept **confidential**, **sharing** them is **cheating**. No distinction will be made between those who cheat and who facilitate cheating by revealing their submissions.