Lab 9: DNS and DHCPv4

Server System Management - Windows Server Labs

SERAFIM CIOBANU

Academic Year: 2022-2023

Table of Contents

[Introduction 3](#_Toc133922359)

[Learning Goals 3](#_Toc133922360)

[Knowledge (what you need to know) 3](#_Toc133922361)

[Abilities (what you need to be able to do) 3](#_Toc133922362)

[Requirements 3](#_Toc133922363)

[Part 1: DNS 4](#_Toc133922364)

[Part 2: DHCP 8](#_Toc133922365)

[Part 3: Setting things back to normal 10](#_Toc133922366)

## Introduction

In this lab, we’ll look at how a DNS and DHCPv4 server can be implemented and configured in an Active Directory domain. You’ll learn why a DNS server is required for the domain to work, and how it can influence your access to the internet. You’ll also learn how DHCP can be used to automatically configure the network settings for the hosts attached to the network.

## Learning Goals

# Knowledge (what you need to know)

* What is a DNS server, and how does it work?
* What is a DNS forward or reverse lookup table? What record types can be found in these tables?
* How can the DNS server be circumvented, and what role does the hosts file play?
* What is a DHCPv4 server, and how does it work?
* What settings can the DHCPv4 server assign to its clients?

# Abilities (what you need to be able to do)

* Install, configure and troubleshoot a DNS server in an Active Directory domain.
* Configure the DNS server’s forward and reverse lookup tables with the appropriate records.
* Install, configure and troubleshoot a DHCPv4 server in an Active Directory domain.

## Requirements

Your three virtual machines in an active directory domain, as configured in the previous labs (lab 1 and 3 are essential)

* Windows Server 2022 with GUI
* Windows Server 2022 Core
* Windows 11 client

## Part 1: DNS

1. Start your Windows GUI server and Windows 11 VMs (the Windows core server is optional for now but will also be needed later). Sign in to the Windows 11 VM using your personal domain user account and open a local PowerShell console with elevated privileges (do not use PowerShell ISE here).
2. Use a legacy Windows command (+ the necessary parameter(s)) to show the complete IP configuration of your Windows 11 VM, including the information about its DNS and DHCP servers. Paste a screenshot of the output of your command below. What machines act as DNS and DHCP server?

ipconfig /all

A screenshot of a computer

Description automatically generated

As DNS – the GUI server

Default DHCP – well, we do not really have a DHCP server, or VMware would act as one if we would be to actually have an IP assigned

1. Use a legacy command to look up the IP addresses of the following machines:
   * [www.google.com](http://www.google.com)

A computer screen shot of a black screen

Description automatically generated

* + Your GUI Server VM (by using its **GUI-<name>** name)

A screenshot of a computer

Description automatically generated

Paste a screenshot of your command and its output here.

The first two lines of this command’s output should show the name and (IPv4) address of the DNS server. Note that - for now - only the IP address of the DNS server is known, not its name. Also, note the “non-authoritative” answer for [www.google.com](http://www.google.com). We’ll come back to both of these observations later.

For each machine, the command also shows the full name of the requested host. In the case of the GUI server, that full name consists of the hostname, followed by the domain name. What letterword is often used to describe this full name? For what expression is this letterword an abbreviation?

FQDN – Full Qualified Domain Name

1. Repeat questions 1 and 2 in a local PowerShell console on your host machine (non-Windows machines may require alternative commands). Can you find the IP addresses of both machines? Did you expect this? Explain why (not)?

I guess I can only see information regarding the VMnet8 which is the DHCP engine regarding the giving of the IP address.

1. In a previous lab you promoted the GUI Server to be the Domain Controller by using the Active Directory installation wizard. This also automatically configured this machine as the AD domain’s DNS server. Additionally, **two DNS forward lookup zones** were created:

* a zone reserved for Microsoft services (name starting with an underscore)
* a zone corresponding to your domain

On your Windows 11 VM, open the DNS Manager console and connect it to your domain’s DNS server. Do you see both Forward Lookup Zones? Paste here a screenshot with the information for your domain’s forward lookup zone, and the DNS records contained therein.

Yes, you can see both

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

The forward lookup zone contains 4 different DNS record types[[1]](#footnote-2) (check the “Type” column). Note these types here, along with their corresponding abbreviations:

* SOA ( Start of Authority )
* A ( Host )
* NS ( Name Server )

The Host records in the **DNS forward lookup** zone allow retrieving the IP addresses of the hosts in the domain, based on their DNS name (remember question 2).

1. Check in the DNS manager whether a **DNS Reverse Lookup Zone** exists for your domain. Paste a screenshot below.

A screenshot of a computer

Description automatically generated

1. While a **DNS *forward* lookup zone** is used in regular DNS queries to translate a hostname to an IP address, **DNS *reverse* lookup zone**s are used to perform *reverse* DNS queries (IP address to hostname translation).Test this on your Windows 11 VM with the same legacy command you used in question 2, but now use the GUI server’s IP address as a parameter instead of its hostname.

Paste below a screenshot of your command and its output. What name does it return?

A screenshot of a computer

Description automatically generated

It says question 2, but question 2 is about ipconfig, so I think the teacher means question 3, because check DNS record. Forward one works, but the Reverse one does not.

1. Use the DNS manager console to add an IPv4 reverse lookup zone for your subnet (192.168.x.0/24) to the DNS server. Is this sufficient to allow reverse DNS queries?

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

It does not seem to help

A computer screen with white text

Description automatically generated

1. Now we’ll finish configuring the reverse lookup zone by adding the necessary record(s) that identify our domain machines. What new type of record (+ abbreviation) is used in the reverse lookup zone?

PTR = Pointer records

These records can be added in 2 ways: manual or automatic.

* Use the DNS manager console to manually add a record for the Windows 11 VM to the reverse lookup zone. Please note: do not use the browse button to enter the hostname, but type in the FQDN itself!

 get the FQDN via nslookup, then add it to the Reverse Lookup Zone, right-click>new pointer>address and FQDN

* You can also automatically add a host’s DNS record to the reverse lookup zone by running the ipconfig command on that host, with a special option/parameter. What option do you need to use for this? (check ipconfig /?). Use this method to automatically add the GUI server and Core server to the DNS reverse lookup zone of your domain. Write down the command you entered for one of these 2 servers below.

 to do this, you can run ipconfig /registerdns

Note that this command would not work for the Windows 11 VM because it has obtained an IP address from the VMware DHCP server and the latter does not allow dynamic DNS updating.

A screenshot of a computer screen

Description automatically generated

* Paste below a screenshot of your reverse lookup zone, containing the 3 added records.

A screenshot of a computer

Description automatically generated

1. Because we now have a reverse lookup zone, the reverse query from question 7 should be possible. Prove this by pasting a screenshot of this command (run this on your Windows 11 VM) and its output.

A screenshot of a computer screen

Description automatically generated

Note that the DNS server’s name should also no longer be shown as “unknown”.

A screenshot of a computer

Description automatically generated

It is now known, GUI server

1. Even though your DNS server’s lookup zones don’t explicitly contain records for the [www.google.com](http://www.google.com) website, we’ve seen that it still resolves an IP address (question 2). How is this possible? Remember the special way in which you configured a DNS forwarder for your GUI server in the previous labs.

This is also the reason why the DNS lookup command returns a so-called “non-authoritative answer”.

1. In the previous commands you used nslookup in its non-interactive mode. If you are planning to run multiple DNS queries in succession, it can however be interesting to use the interactive mode. Test this in the following way:

* Enter the **nslookup** command without arguments. This starts the interactive mode.
* In interactive mode you can execute a number of special commands. List the available commands with the command **help (or ?)**
* Use one of these commands (without additional arguments) to retrieve the DNS server currently used for DNS translations

A black screen with white text

Description automatically generated

* Now use this same command again, but add the IP address of another DNS server as an argument, e.g. the one used by your host (laptop). At home, you can also try the DNS server of Google (8.8.8.8), but if you work at Howest, external DNSes are blocked by the Howest firewall.

A screen shot of a computer

Description automatically generated

* Now request the IP address of [Twitter](http://www.facebook.com/). Please note: in interactive mode you don’t need to type the nslookup command again, just the domain name (or IP address) is sufficient!

A computer screen with white text

Description automatically generated

* Request the IP address of your core server using its FQDN. Why does this no longer work?

A black screen with white text

Description automatically generated

Because we changed the server to 8.8.8.8?

* Type “exit” to close the nslookup prompt.

1. To allow tracking revisions of the DNS lookup zones, each zone’s SOA record contains a “serial number” value that is incremented with every update.

* Use the DNS manager console to find the serial number of the forward lookup zone of your domain. Paste a screenshot of the full window where you found this value.

A screenshot of a computer

Description automatically generated

* Add a new alias record for the GUI server to your domain forward lookup zone, and name it alias-<firstname> (e.g. alias-thomas). Paste a screenshot of the new record.

right-click>new alias

A screenshot of a computer

Description automatically generated

* Due to this adjustment, the serial number of the SOA record should be increased by (at least) one. Check this! (you may need to refresh the DNS data to see the increment)

A screenshot of a computer

Description automatically generated

1. When a host performs a DNS lookup, it (temporarily) saves the results in its local DNS cache to potentially improve the performance of future queries.

* Use a legacy Windows command on the Windows 11 VM to show the contents of the local DNS cache. Write down the command here:

 ipconfig /displaydns

A screenshot of a computer

Description automatically generated

* Now use the same legacy command (with a different parameter) to clear the contents of the local DNS cache.  Write down the command here:

 ipconfig /flushdns

A screen shot of a computer program

Description automatically generated

* Repeat the first command to check whether the DNS cache is indeed empty.

A screenshot of a computer

Description automatically generated

It is not empty for some reason, but I suppose it would normally work.

* Ping to the alias-<firstname> name you configured in the previous question. Check the contents of the local DNS cache after the ping and paste a screenshot here. Can you find information for **alias-<firstname>**?

A computer screen with white text

Description automatically generated

A screenshot of a computer

Description automatically generated

Yes, you can

* What is the TTL value of the record in your DNS cache? What does this value mean?

 3585

 Indicates how long the DNS record is valid and should be retained in the cache before it needs to be refreshed from the DNS server

* The TTL value changes over time. What do you think was its initial value?

 3600

 Why? Because 3600 (seconds) / 60 = 60 minutes. I guess it is some default time after which the DNS record should be renewed

* Check your predicted answer using the DNS Manager console and paste a screenshot of this setting below. Hint: use the Advanced View!

A screenshot of a computer

Description automatically generated

1. Because the GUI server acts as a DNS server/forwarder for the domain, external lookups by the Windows 11 VM will also be cached on the server. This is called server-side DNS cache. Test this as follows:

* Surf (or ping) to [www.tijd.be](http://www.tijd.be/) **from your Windows 11 VM**
* Check with DNS Manager if you find traces of the address translation in the server-side DNS cache. Hint: use the Advanced View! (you may again need to refresh the DNS data)

A screenshot of a computer

Description automatically generated

Indeed it works.

1. For some applications suchw as e.g busy web servers, it can be useful to distribute requests over multiple servers (load balancing). One possible way to implement this, is by using “round robin” DNS resolution.

* Check with DNS Manager if your DNS server supports Round Robin. Paste below a screenshot of the window where you found this setting.

 Server>right-click>Properties>AdvancedA screenshot of a computer

Description automatically generated

* Test the Round Robin setting as follows:

* Add 2 new (IPv4) Host records to the DNS server, and use the same name for both records (use **<your first name>**, e.g. Thomas). Link the first host record to the IP address of your GUI server and link the second host record to the IP address of your Core server.

A screenshot of a computer

Description automatically generated

* Ping **<your first name>**. Normally, this will ping the first IP address, associated with this name (i.e. the address ending at 100).

A computer screen with white text

Description automatically generated

* Ping <your first name> again. Normally, because of the Round Robin setting, this time the second IP address should be pinged (i.e. the address ending at 101). Why does this not happen, and does the first address get pinged again?

Probably happens because of DNS caching

* What command do you need to type to avoid this?

ipconfig /flushdns

nslookup Serafim

ping Serafim

* If you ping to your first name again after doing this, the second IP address should now get pinged. Paste a screenshot with both ping commands and the intermediate command

A screenshot of a computer program

Description automatically generated

1. To improve the security of the DNS queries and protect them against DNS spoofing/poisoning, a protocol called DNSSEC can be used. Check whether this is enabled for your domain and paste a screenshot of where you found this. Please note: Don't change this setting!

A screenshot of a computer

Description automatically generated

Enabled

1. DNS clients typically also have a “hosts” file that can locally override hostname-to-IP address translations. All translation that can be found in this file are automatically (and permanently – at least until the hosts file is modified) loaded into the client’s DNS cache, so that queries for these translations are no longer sent to the DNS server. Proceed as follows to test this (and thus “poison your DNS cache”):

* Add an extra line to the hosts file on your Windows 11 VM so that the name of the (existing!!) [website](http://www.serverlabs.be/) www.serverlabs.be is translated to the IP address **172.217.168.206**. Don't forget to save the changes!

Here is the default we see

A screenshot of a computer

Description automatically generated

* Paste below a screenshot of the custom content of your hosts file.

A screenshot of a computer

Description automatically generated

* Surf on your Windows 11 VM to www.serverlabs.be

A computer screen shot of a computer screen

Description automatically generated

* Surf on your GUI server to the same website. Do you see the same content?

A screenshot of a computer

Description automatically generated

In my case it did not work, but what it would have to do, is probably show the same content.

Do not forget to afterwards comment out (or remove) the extra line you added to the hosts file!

## Part 2: DHCP

1. In question 1, we used a legacy Windows command to get information about the network connection of the Windows 11 VM. Now combine this command with the findstr command to limit the output to the lines with the following information and paste a screenshot of the commands and their output (use a separate parameter combination for each line):
2. The IPv4 address

ipconfig | findstr /R "IPv4"

A black screen with white text

Description automatically generated

1. Did the NIC receive the IPv4 address from a DHCP server?

ipconfig /all | findstr /C:"DHCP Enabled"

A black screen with white text

Description automatically generated

1. What is the IP(v4) address of the DHCP server?

 ipconfig /all | findstr /C:"DHCP Server"A computer screen shot of a computer

Description automatically generated

We do not have a DHCP Server

All we have is default gateway, and the IP addresses were set manually. The DHCP server is supposed to either be the VMNet8, or the GUI server when set up

But considering the default gateway, we can say that the DHCP server is 192.168.206.254 according to the note.

it might be because I had to disable the service prior to it for the other labs like Lab 9 Linux, so maybe the situation would be different

Note that the DHCP server’s IP is the last IPv4 host address in the VMnet8 subnet!

1. In this part of the lab, we do not want to use the DHCPv4 server of VMware Workstation. Therefore, you first need to **disable the VMware DHCP service** on your host machine. Do this!

A screenshot of a computer screen

Description automatically generated

Please note: Don't forget to reactivate this service after the lab! After all, you will also use VM’s for other modules that use this service!

1. Now use a legacy Windows command (and its appropriate parameters) to:

* release the IP address configuration on your Windows 11 client

ipconfig /release

* refresh the IP address configuration on your Windows 11 client. This may take a long time since your NIC tries to contact a non-existing DHCP server, but wait until you get an error message.

ipconfig /renew

* What kind of IPv4 address did the client’s NIC now receive? (remember the Computer Networks course). How do you know this?

169.254.x.y – APIPA (Automatic Private IP Addressing) kind of things, that is given when there is no authority to give you an IP address.

* Can you still ping from the Windows 11 VM to the (GUI/CORE) servers? Why (not)? Test this!

 You are not supposed to be able to ping to it, as now you are not supposed to have connection to the network where other machines are.

1. Using the Server Manager, install a DHCP Server on your GUI VM (work on the GUI server directly, since connectivity between the Win11 and GUI machines is now temporarily lost).

Note: in production systems, Microsoft typically recommends to avoid installing a DHCP server on a domain controller, because any added services may introduce additional bugs and attack vectors to the machine. Given the DC’s importance in managing the domain, it should thus run only the core services required.

A screenshot of a computer

Description automatically generated

Do not forget to click on the blue link “Complete DHCP configuration” after installation. This will allow you to configure your GUI server as an authorised DHCP server within your domain.

A screenshot of a computer

Description automatically generated

1. Open the DHCP management console and add a new IPv4-scope with the following features:

Tools>DHCP

A screenshot of a computer

Description automatically generated

Right-click IPv4 > New Scope

* Name: your first name
* Start IP address: 192.168.x.40
* End IP address: 192.168.x.50
* Subnet mask: default setting
* Do not add Exclusions or delays
* Lease duration: default setting
* DHCP scope options: default settings
* Gateway: the default gateway of your VMnet8 network
* Parent domain: default settings
* DNS Server: your domain controller (GUI server)
* Do not specify WINS Server
* Activate your scope

Now add your DNS server and your DNS domain name as DHCP server options.

A screenshot of a computer

Description automatically generated A computer screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A computer screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Check in your DHCP management console if your DHCP server has already distributed IP addresses.

If this is not (yet) the case: refresh the IP address configuration on your Windows 11 VM again!

 Had to disable manual network settings (via gui in Settings>Network and Internet>Ethernet>IP assignment>Automatic

NOTE: Probably had to do the same thing when we were checking for DHCP being enabled in the other question prior here.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Write down the “unique ID” associated with the distributed IP address in the DHCP console. What information is shown here? (tip: write down the hexas in groups of 2 and think of the Computer Networks course).

A computer screen shot of a computer

Description automatically generated

 00 0c 29 d5 82 dc

A screenshot of a computer

Description automatically generated

It is the MAC address of the NIC that received the IP address.

1. Change the lease time from 8 to 20 days

Paste below a screenshot of the full window in which you did this.

A computer screen shot of a computer

Description automatically generated

1. Refresh the IP address configuration on your Windows 11 VM and then prove with a command line that the lease time is now set to 20 days (paste a screenshot here).

ipconfig /release

ipconfig /renew

Tip: limit the the output of the ipconfig/all command to the 2 lines with Lease-info.

 ipconfig /all | findstr /C:"Lease"

A screen shot of a computer

Description automatically generated

1. Now configure the DHCP server in such a way that it always assigns the IP address 192.168.x.77 to the Windows 11 VM.

DHCP Console > Scope > Reservations > Right-click > New Reservation

A computer screen shot of a computer

Description automatically generated A screen shot of a computer

Description automatically generated A screenshot of a computer

Description automatically generated

Check if your Windows 11 VM will indeed be assigned the reserved IP address. Of course, you must first release the IP address that is currently in use.

Also check that this new address has been added to the DNS database of your DNS server. Paste a screenshot of the corresponding DNS record in the forward lookup zone.

A computer screen shot of a computer

Description automatically generated

## Part 3: Setting things back to normal

1. To finish, we’ll set the DHCP settings back to normal, so we don’t interfere with any other virtual machines:
   1. De-activate the IPv4-scope that you defined in question 23. The DHCP server now has no more IP addresses it can assign to another machine, so it will become inactive.
   2. re-activate the VMware DHCP service on your host (important!)
   3. Check if the VMware DHCP service works by renewing the IP address of the Win11 VM.

A screenshot of a computer

Description automatically generated

Now I do not have manual IP set on the WIN11, and not manual as I had for all the labs from the very beginning

1. If IPv6 is not enabled in VMware, there may only be 3 types of DNS records. One of the types is IPv6 specific. [↑](#footnote-ref-2)