
# Project Technical Document
# Subject: Preconfigured Network Infrastructure and Security Implementation Using GNS3

Narges Ghabezi
Group Name: CyberSentinel

*Department of Computer Science*
*New York Institute of Technology*

*Professor Dr. Sara Khanchi*

*Fall 2023*
Vancouver, Canada

**Table of Contents**

13. Network Monitoring / Netwatch configuration
  - Function Verification
14. Networker Toolkits as FTP/TFTP Server/ Web Server / Syslog Server,SNMP Trap receiver
    - Importing the Networker Toolkits
    - Internet connection verification
  - WebTerm Installation
  - Xfe file manager
15. FTP Server connection
  - Uploading file to FTP Server
16. TFTP Server/Client installation
  - Uploading file to TFTP Server
17. Remote Syslog Server
  - Configuring Mikrotik to log into remote Syslog Server
  - Adding Action
  - Adding syslog rules
  - Log Verification
18. Final Topology Diagram
19. Conclusion
20. References
21. Appendix: Troubleshooting Virtualization Issues.

## Introduction

The utilization of Cisco IOS Routers in the GNS3 environment, especially Cisco devices, has financial implications as they are not freely accessible. While there are alternative vendors such as Cumulus or Arista, their compatibility can be a hassle. This report addresses the objective of creating a free, preconfigured virtual router within the GNS3 environment. By implementing the MikroTik Cloud Hosted Router, leveraging its advanced capabilities in virtualized networking, routing, and security.

## Objective

The report primarily focuses on providing a detailed manual for creating objects, outlining their features and associated problems, and offering solutions. It emphasizes the importance of installing and utilizing GNS3 with VMware Player, a recommendation made based on the author's experience with other virtualization solutions like Virtual Box and Virtual Router. VMware Player is suggested due to its non-commercial free availability and superior capabilities. GNS3 VM, is highlighted as crucial for emulating network devices in a QEMU virtual environment. It offers enhanced performance and stability compared to running GNS3 directly on the host operating system, enabling the creation of complex network topologies without overwhelming the host machine's resources.

## Technical Requirements

The recommended specifications for the hosted machine should be sufficient.

GNS3 VM Requirements on Windows host:
- Dual-core processor or higher.
- Intel VT-x or AMD-V virtualization extensions (should be enabled in the BIOS/UEFI. (1.4 GHz 64-bit processor or faster.)
- RAM: Minimum 2GB
- MikroTik CHR: 256 MB RAM
- Ubuntu Docker Containers (each): 128 MB RAM
- Servers running on Ubuntu Docker: 256 MB RAM
- Windows servers: 1024 MB RAM
- Kali Linux: 256 MB RAM
- Windows Server 2012: 2G RAM
- hard disk for total project: 30G (Optimal)

Below is a detailed walkthrough for installing GNS3 with VMware Player as GNS3 VM:

To set up GNS3 using VMware Player as a GNS3 VM, you'll need to install various applications and components. Here's the list of required software:

1. **VMware Player**
   - virtualization application (Similar to Virtual Box)

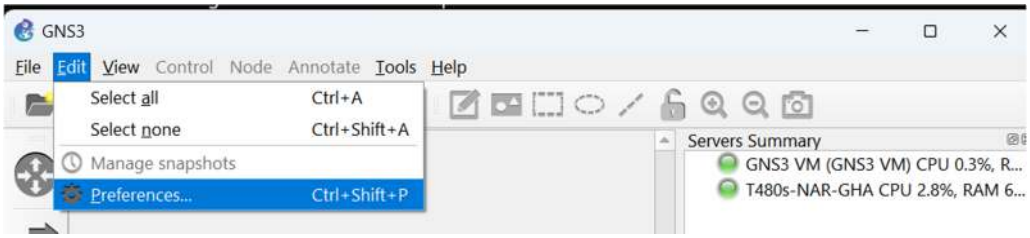
https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html

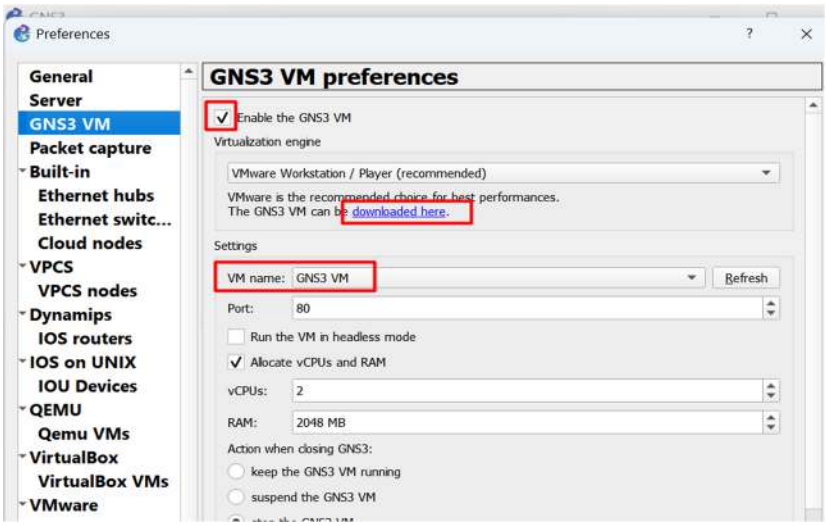

2. GNS3 (network simulation software)

https://gns3.com/software/download

3. GNS3 VM:

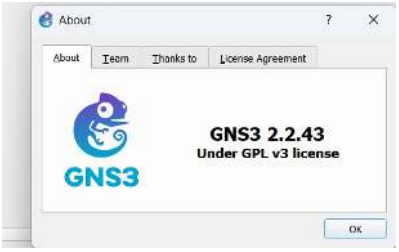
Download the GNS3 VM image from within the GNS3 application. Go to `Edit > Preferences > GNS3 VM` and follow the prompts to download and import the GNS3 VM.



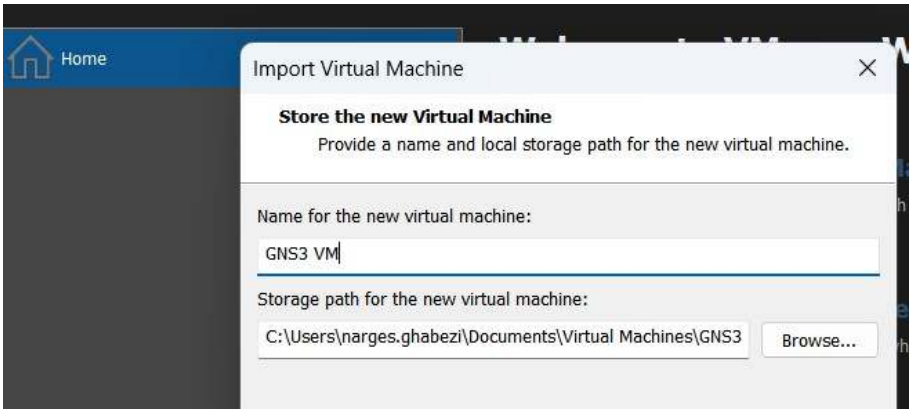
Alternatively, you can download it directly from the official GNS3 website, tailored to your specific virtualization platform.

**Note: Make sure the GNS3 Machine and GNS3 VM are same version.**

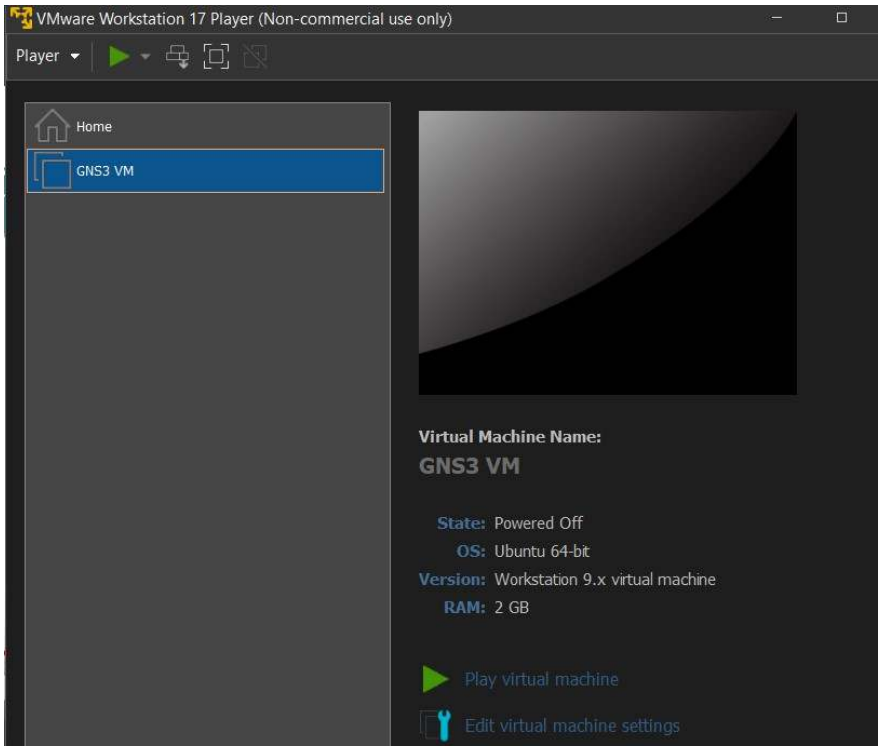



Next, you must import the GNS3 VM, which comes in the form of a .ova file.


Ensure that the virtual machine is named "GNS3 VM" and do not opt for any other name.

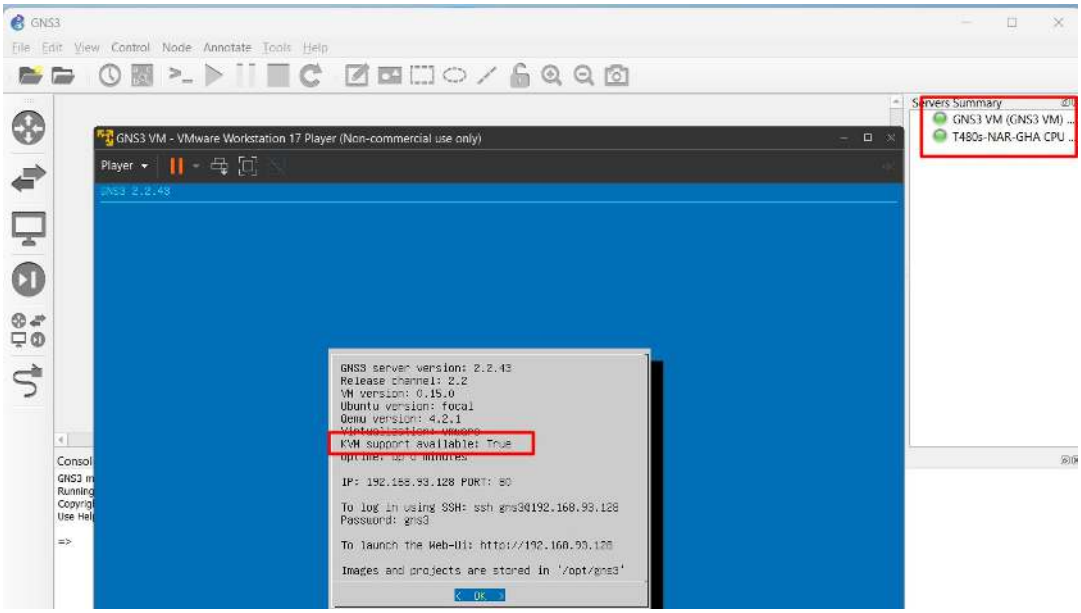



After importing the virtual machine, you will be presented with its specifications and settings.

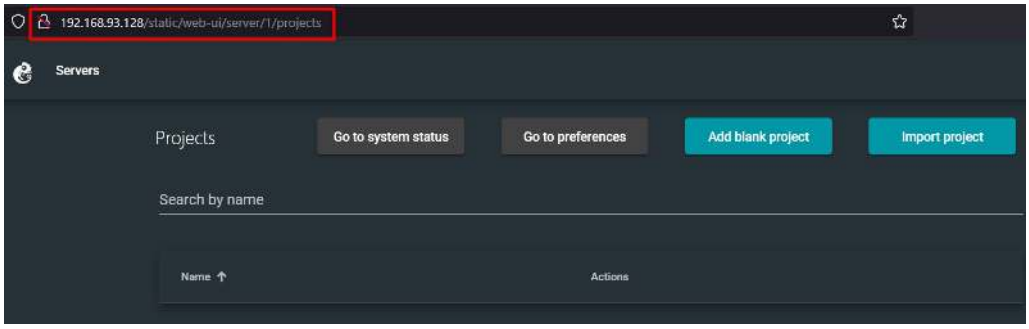



From here When you open GNS3 on your host machine, the software checks the configuration settings to see if it's integrated with a GNS3 VM if yes it will turn the Machine On for you.

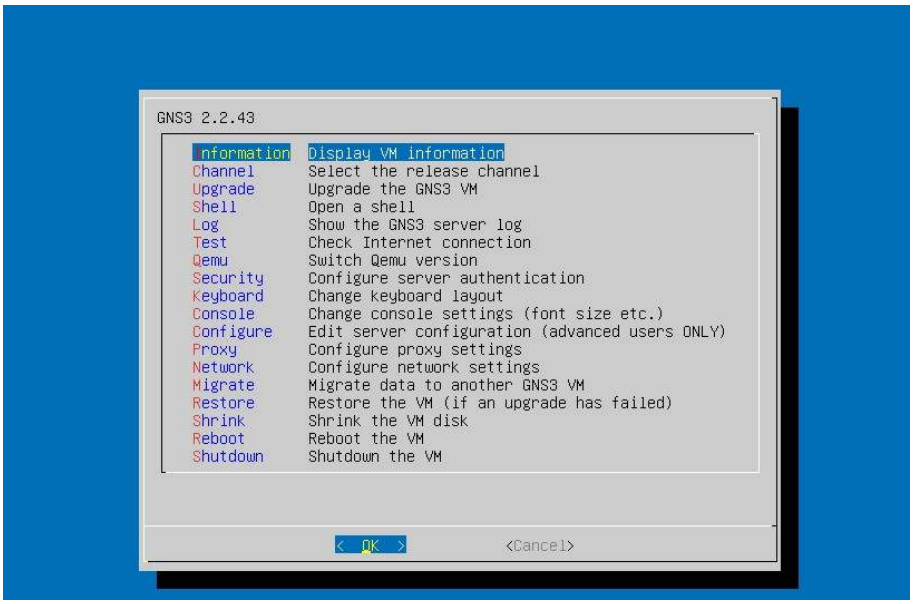
If the configuration is correct, you should observe that the services are operational and indicated by green status indicators. Specifically, for the Qemu environment, ensure that the "KVM Support Available" status is marked as True. If it is not true, refer to the Appendix for instructions on how to enable it.



Moreover, you can establish a connection to the GNS3 VM on Port: 80 through the provided IP address.



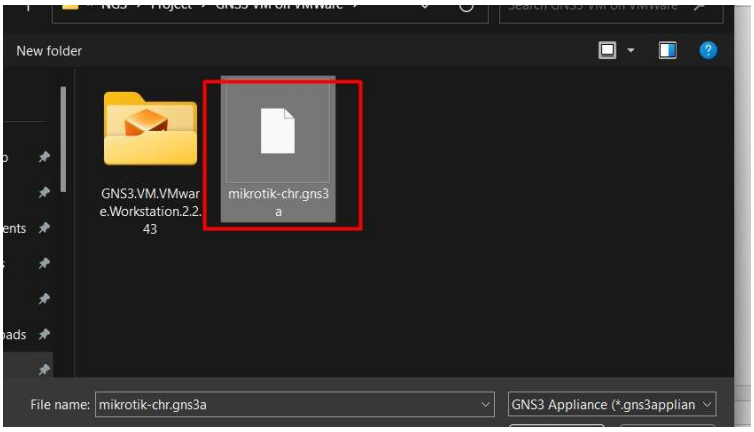

At this point, you'll gain access to additional features, including the ability to switch to the Qemu version, view logs, and manage security settings.



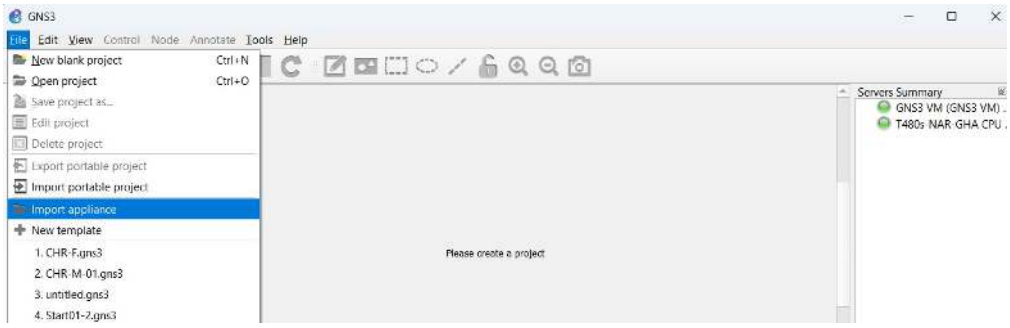

Setting up the appliances involves importing them. In this section, I'll demonstrate how to import an appliance, which requires an application image. Additionally, I'll explain how to import your custom template if the version or device you're looking for isn't available in GNS3.Importing Appliance:

**Method 1: Using GNS3 Appliance Marketplace**

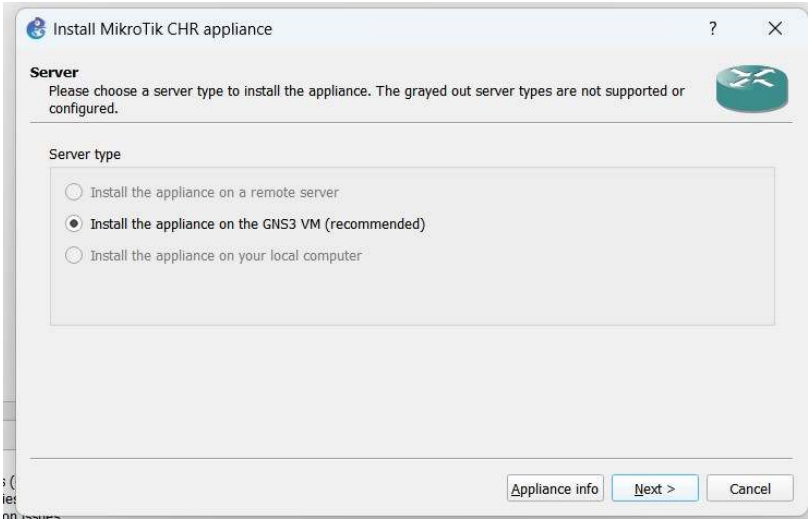
Go to GNS3 Marketplace from the main interface, download the appliance file (usually in OVA or QEMU format) with a .gns3 extension, specifically opting for the CHR Mikrotik appliance in this case. Alternatively, you have the option to download the GNS3 appliances from this source. https://www.gns3.com/marketplace/appliances.




**Import Appliance into GNS3:** Click on "File" in the menu bar and select "Import Appliance..."

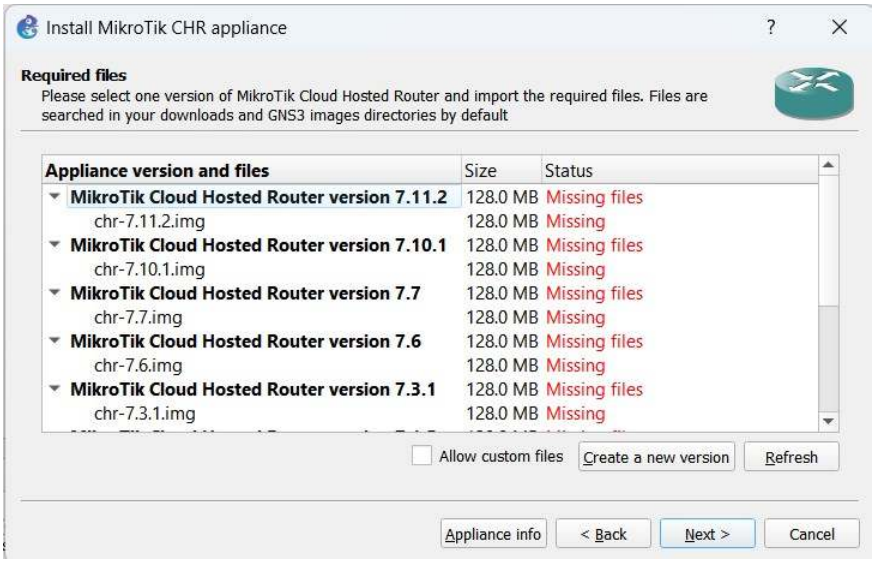



Select your server preference: We will opt for GNS3 VM and advanced tools, specifically designed to function within the GNS3 VM environment utilizing Qemu virtualization.

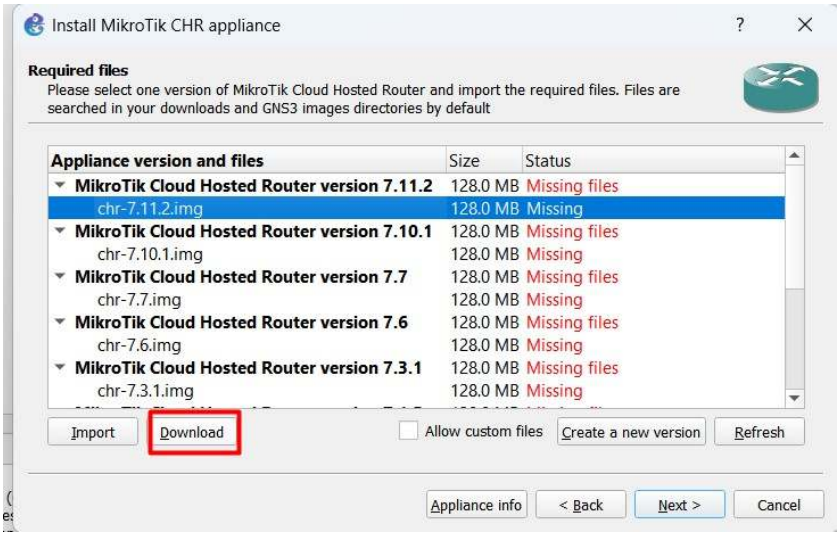


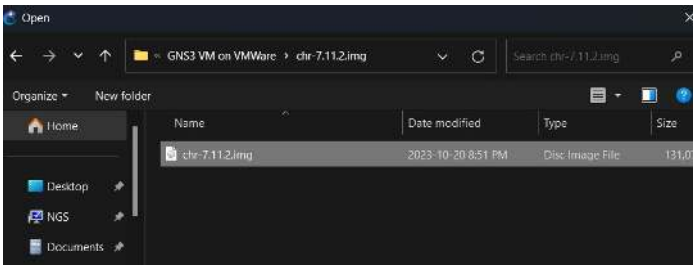
Select the default Qemu binary and allow GNS3 to make the choice for you.


In this step, you'll require the .img file of the desired appliance you wish to install. If the appliance isn't listed, you have the option to create your own template by selecting "New template."

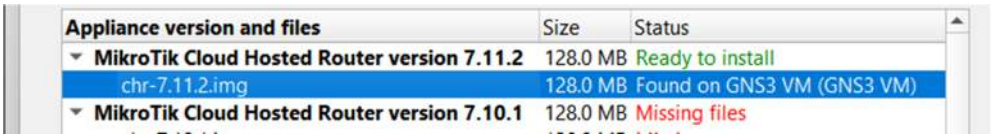



Click on the preferred CHR or appliance version. You can either download it or import it if you already have the file on your system. Ensure the file has been unzipped beforehand.



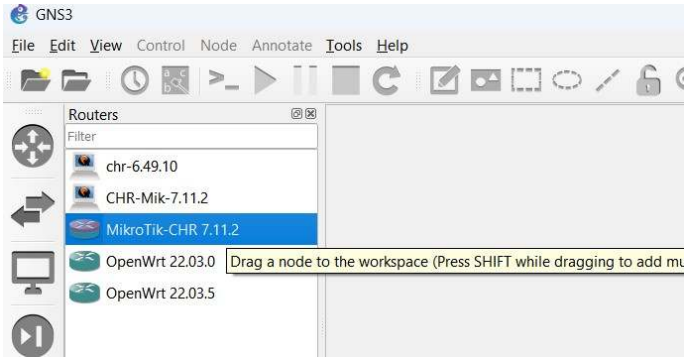



The status indicator should turn green to indicate successful completion.

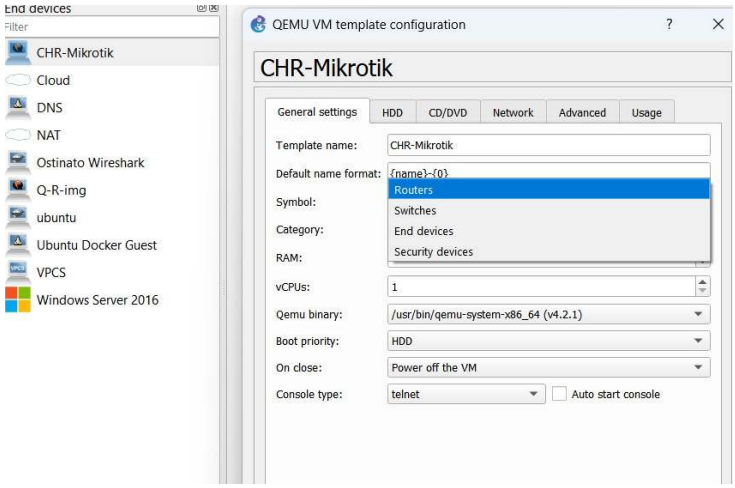



Proceed by accepting and approving the installation.

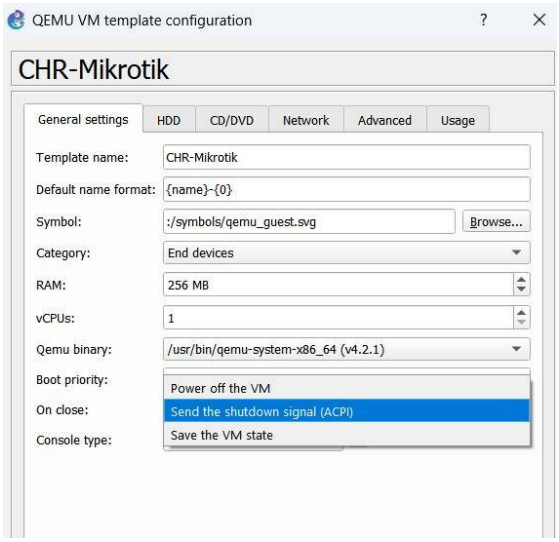

Your device or appliance is now prepared and available in the GNS3 Devices list, ready to be dragged and integrated into your network topology.




If you have imported the image manually, you can modify the configurations to ensure the device is visible under Router devices.



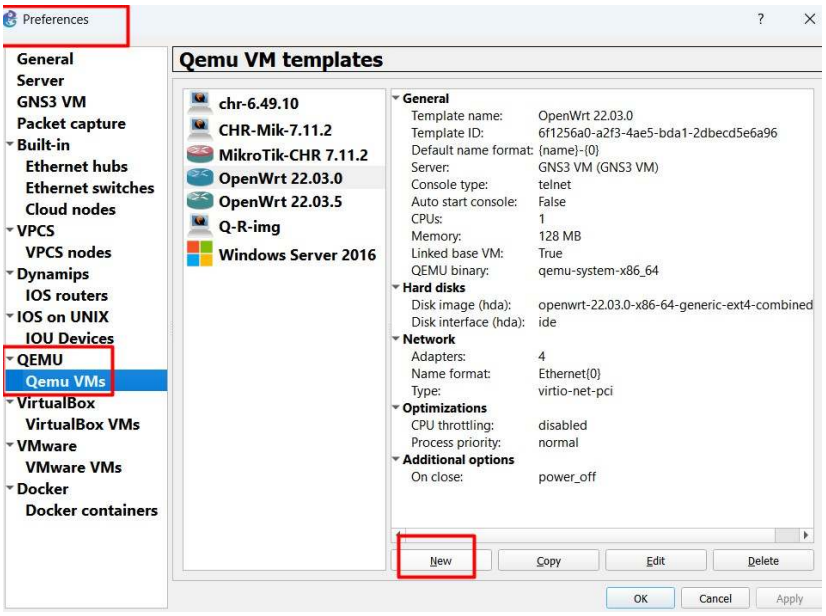

It is strongly advised to configure the "on close" action to send the shutdown signal (ACPI) for proper system management.




**Method 2:** Method 2 involves creating your own template or an alternative method for adding the appliance image file.

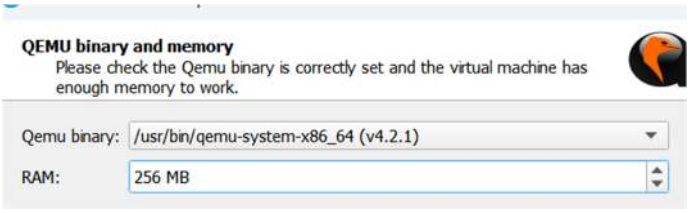
1. Navigate to GNS3 > File > Preferences.

2. Select your preferred virtualization environment. For this demonstration, Qemu VM is chosen. (Note: For Docker environment, select Docker VM.)

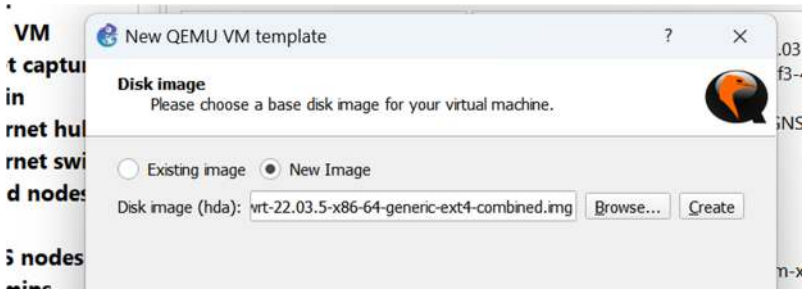



Select the appropriate server type:

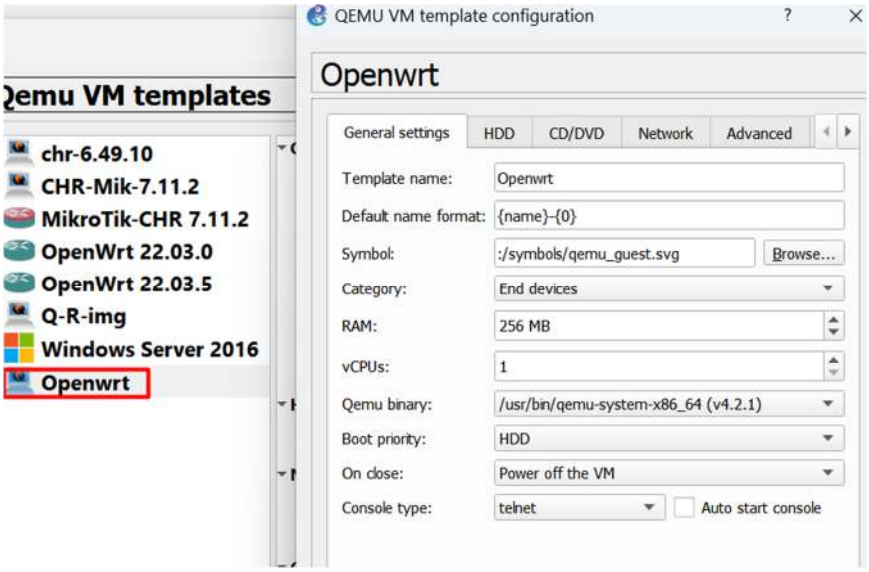

Configure the Qemu binary and memory settings as follows:




Upload the desired appliance image. For instance, in this demonstration, I used the Openwrt .img file.(sample img you can have your own desired .img file)



Once the appliance is added, you can customize the image according to your specific requirements.



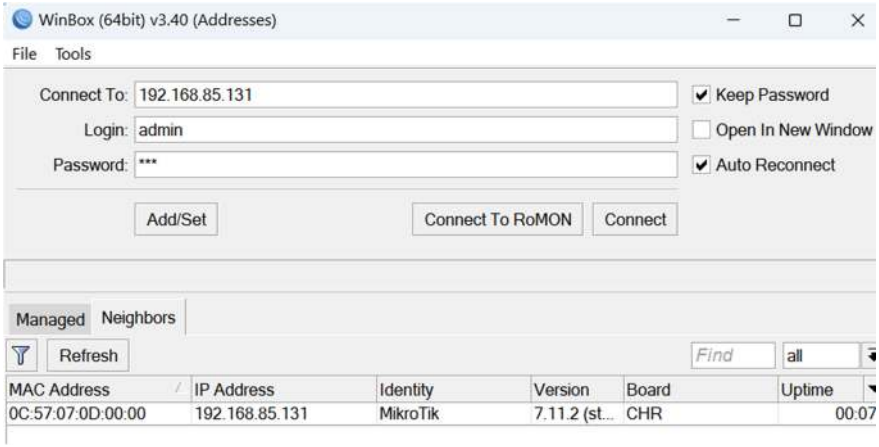

The device is now prepared and ready to be added to your network topology.

With the environment prepared, I will proceed to create the network topology and configure it accordingly.

**How to use Winbox to get access to GUI of the CHR Mikrotik Router.**

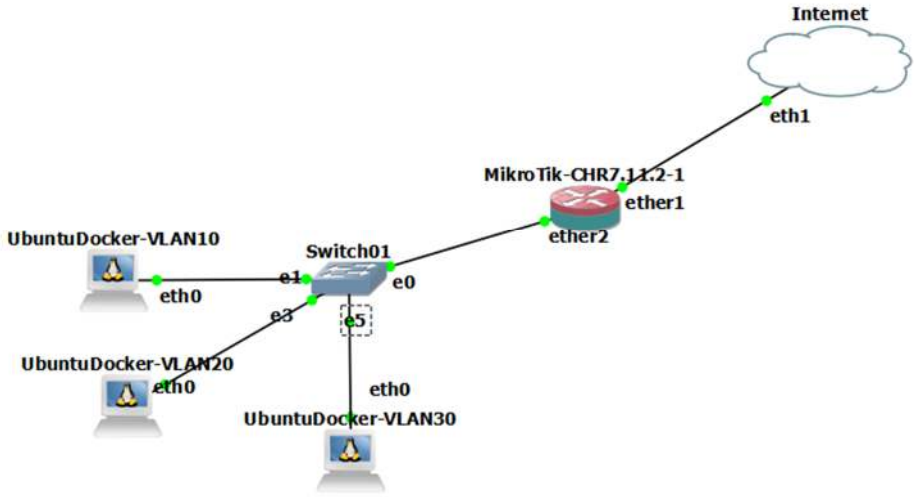
Download and install Winbox : https://mikrotik.com/download

Double-click the Winbox executable file to launch the application. Winbox can automatically discover MikroTik devices on your network. If the CHR router is on the same local network as your computer, Winbox should be able to find it without manual configuration. Click on the "**Neighbors**" tab in Winbox, and it will display a list of MikroTik devices found on the network.

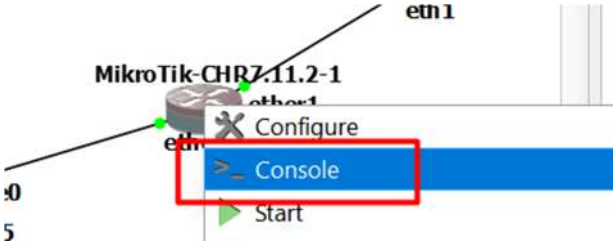


**How to turn on and get access to the CLI environment of the CHR Router:**

Once devices have been added to your network configuration, you can activate them and access their consoles. GNS3 provides built-in tools like Console, and external applications such as Solar Putty, ensuring seamless connectivity to device interfaces.




After the device has been restarted, simply right-click on it and initiate the console.




I will provide the configuration using both the Command Line Interface (CLI) and the Winbox Graphical User Interface (GUI).

**Configure Cloud Hosted Router interfaces:** *(Note: The interface configuration may vary depending on your specific network settings.)*

**Eth0 = Wired / Eth1 = Wireless (***I was getting internet connection on my Wi-Fi on Eth1)*

- **Display the interface**:

*#interface print*

```
[admin@MikroTik] > interface print
Flags: R - RUNNING
Columns: NAME, TYPE, ACTUAL-MTU, MAC-ADDRESS
#    NAME    TYPE   ACTUAL-MTU  MAC-ADDRESS
0  R ether1  ether        1500  0C:5C:5E:86:00:00
1    ether2  ether        1500  0C:5C:5E:86:00:01
2    ether3  ether        1500  0C:5C:5E:86:00:02
3    ether4  ether        1500  0C:5C:5E:86:00:03
[admin@MikroTik] >
```

- **IP Address Print**

*# ip address/ print*

```
[admin@MikroTik] > ip address/ print
Flags: D - DYNAMIC
Columns: ADDRESS, NETWORK, INTERFACE
#    ADDRESS            NETWORK        INTERFACE
0    10.0.100.1/24      10.0.100.0     ether2
1    10.0.10.1/24       10.0.10.0      vlan10
2    10.0.20.1/24       10.0.20.0      vlan20
3    10.0.30.1/24       10.0.30.0      vlan30
4 D 192.168.85.131/24   192.168.85.0   ether1
[admin@MikroTik] >
```

- **Setting IP address for the interfaces.**

*#ip address add address=<ip_address>/<subnet_mask> interface=<interface_name>*

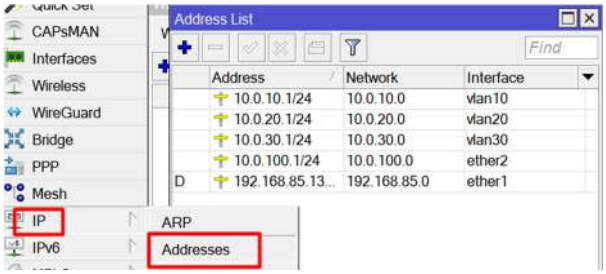
*# ip address add address=10.0.100.0/24 interface=ether2*

- **Remove IP address.**

*#ip address remove [find address="IP/Subnet"]*

```
Password changed
[admin@MikroTik] > ip address/ print
Flags: D - DYNAMIC
Columns: ADDRESS, NETWORK, INTERFACE
#    ADDRESS            NETWORK        INTERFACE
0 D 192.168.85.131/24   192.168.85.0   ether1
[admin@MikroTik] > ip address add address=10.0.20.1/24 interface=ether2
[admin@MikroTik] > ip address/ print
Flags: D - DYNAMIC
Columns: ADDRESS, NETWORK, INTERFACE
#    ADDRESS            NETWORK        INTERFACE
0 D 192.168.85.131/24   192.168.85.0   ether1
1    10.0.20.1/24       10.0.20.0      ether2
[admin@MikroTik] > ping 8.8.8.8
  SEQ HOST                                     SIZE TTL TIME       STATUS
    0 8.8.8.8                                    56 128 18ms470us
    1 8.8.8.8                                    56 128 24ms444us
    2 8.8.8.8                                    56 128 18ms29us
    3 8.8.8.8                                    56 128 16ms965us
    sent=4 received=4 packet-loss=0% min-rtt=16ms965us avg-rtt=19ms477us max-rtt=24ms444us

[admin@MikroTik] >
```

**View or add the IP address through Winbox**:




- **Route Print.**

*#IP Route Print*

```
[admin@MikroTik] > ip route print
Flags: D - DYNAMIC; A - ACTIVE; c - CONNECT, d - DHCP
Columns: DST-ADDRESS, GATEWAY, DISTANCE
    DST-ADDRESS       GATEWAY        DISTANCE
DAd 0.0.0.0/0         192.168.85.2          1
DAc 10.0.20.0/24      ether2                0
DAc 192.168.85.0/24   ether1                0
[admin@MikroTik] >
```

- **Create VLAN Interfaces. (VLAN 10, 20,30). This creates three VLAN interfaces named `vlan10`, `vlan20`, and `vlan30` on the `ether2` interface with VLAN IDs 10, 20, and 30 respectively.**

*#interface vlan add name=vlan10 interface=ether2 vlan-id=10*

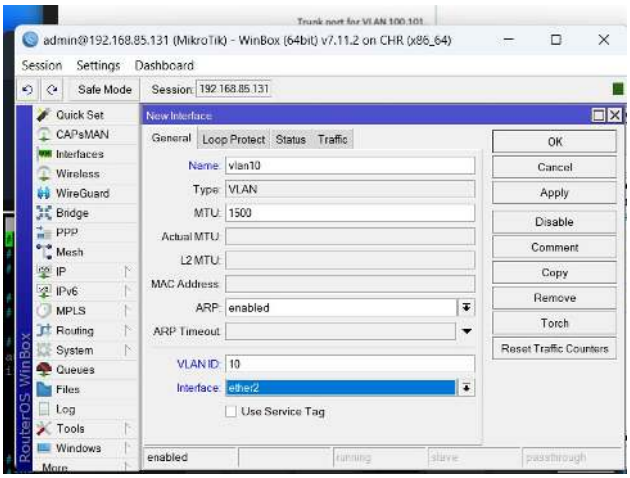
*#interface vlan add name=vlan20 interface=ether2 vlan-id=20*

*#interface vlan add name=vlan30 interface=ether2 vlan-id=30*

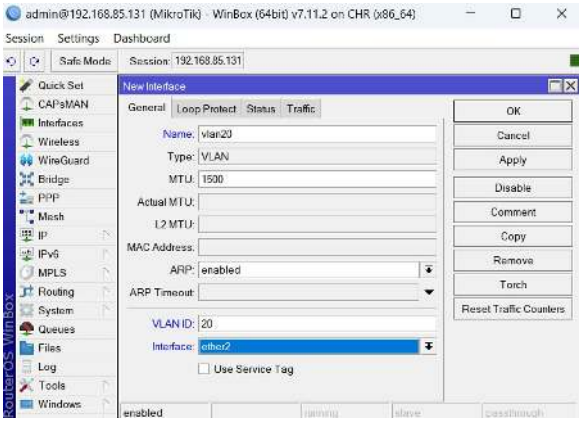
```
[admin@MikroTik] > ip address add address=10.0.100.1/24 interface=ether2
[admin@MikroTik] > interface vlan add name=vlan10 interface=ether2 vlan-id=10
[admin@MikroTik] > interface vlan add name=vlan20 interface=ether2 vlan-id=20
[admin@MikroTik] > interface vlan add name=vlan30 interface=ether2 vlan-id=30
[admin@MikroTik] >
```

**Via Winbox:** *Interfaces > VLAN > Add new interface >*

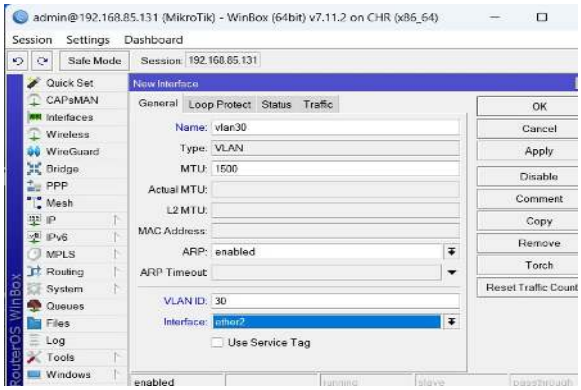
**VLAN 10 on Ether2**




**VLAN 20 on Ether2**




**VLAN 30 on Ether2**




- **Assign IP Addresses to VLAN Interfaces**

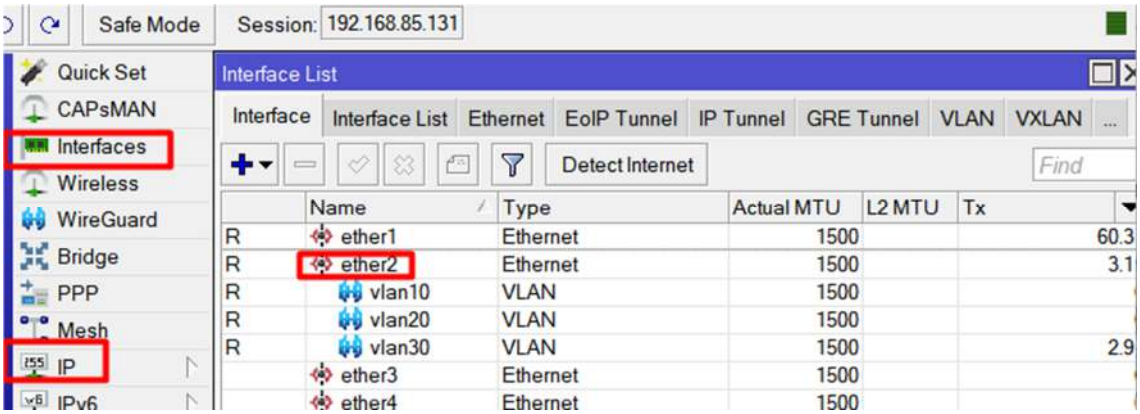
*#ip address add address=10.0.10.1/24 interface=vlan10*

*#ip address add address=10.0.20.1/24 interface=vlan20*

*#ip address add address=10.0.30.1/24 interface=vlan30*

```
[admin@MikroTik] >
[admin@MikroTik] > ip address add address=10.0.10.1/24 interface=vlan10
[admin@MikroTik] > ip address add address=10.0.20.1/24 interface=vlan20
[admin@MikroTik] > ip address add address=10.0.30.1/24 interface=vlan30
[admin@MikroTik] >
```

**Winbox:**




- **Configure DHCP Servers for VLANs**

*#ip dhcp-server network add address=10.0.10.0/24 gateway=10.0.10.1 dns-server=8.8.8.8*

*#ip dhcp-server network add address=10.0.20.0/24 gateway=10.0.20.1 dns-server=8.8.8.8*

*#ip dhcp-server network add address=10.0.30.0/24 gateway=10.0.30.1 dns-server=8.8.8.8*

- **Create DHCP Address Pools and Enable it.**

*#ip pool add name=pool-vlan10 ranges=192.168.10.2-192.168.10.254*
*#ip pool add name=pool-vlan20 ranges=10.0.20.2-10.0.20.254*
*#ip pool add name=pool-vlan30 ranges=10.0.30.2-10.0.30.254*

*#ip dhcp-server add interface=vlan10 address-pool=pool-vlan10 disabled=no*

*#ip dhcp-server add interface=vlan20 address-pool=pool-vlan20 disabled=no*

*#ip dhcp-server add interface=vlan30 address-pool=pool-vlan30 disabled=no*

```
admin@MikroTik] >
admin@MikroTik] > ip dhcp-server network add address=10.0.10.0/24 gateway=10.0.10.1 dns-server=8.8.8.8
admin@MikroTik] > ip dhcp-server add interface=vlan10 address-pool=pool-vlan10 disabled=no
nput does not match any value of address-pool
admin@MikroTik] > ip pool add name=pool-vlan10 ranges=10.0.10.2-10.0.10.254
admin@MikroTik] > ip dhcp-server network add address=10.0.20.0/24 gateway=10.0.20.1 dns-server=8.8.8.8
admin@MikroTik] > ip pool add name=pool-vlan20 ranges=10.0.20.2-10.0.20.254
admin@MikroTik] > ip dhcp-server network add address=10.0.30.0/24 gateway=10.0.30.1 dns-server=8.8.8.8
admin@MikroTik] > ip pool add name=pool-vlan30 ranges=10.0.30.2-10.0.30.254
admin@MikroTik] > ip dhcp-server add interface=vlan10 address-pool=pool-vlan10 disabled=no
admin@MikroTik] > ip dhcp-server add interface=vlan20 address-pool=pool-vlan20 disabled=no
admin@MikroTik] > ip dhcp-server add interface=vlan30 address-pool=pool-vlan30 disabled=no
admin@MikroTik] >
```

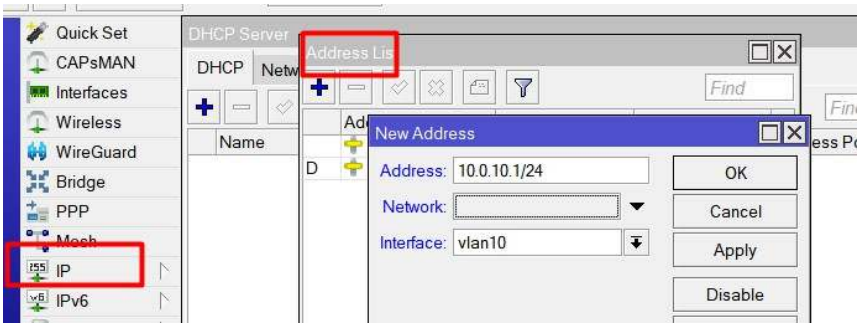
**Verification of the DHCP Settings.**

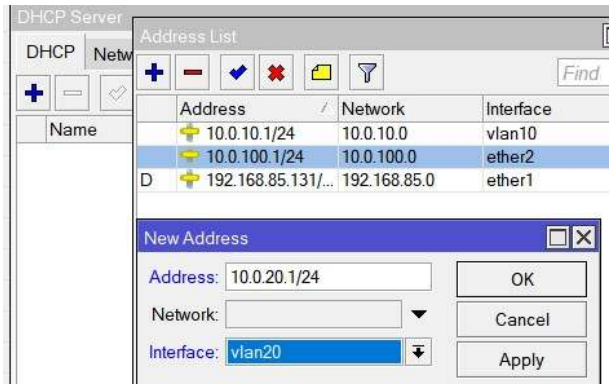
*#ip dhcp-server print*

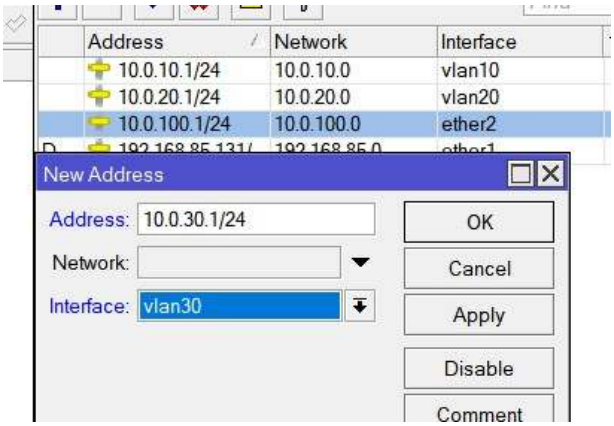
*#ip dhcp-server network print*

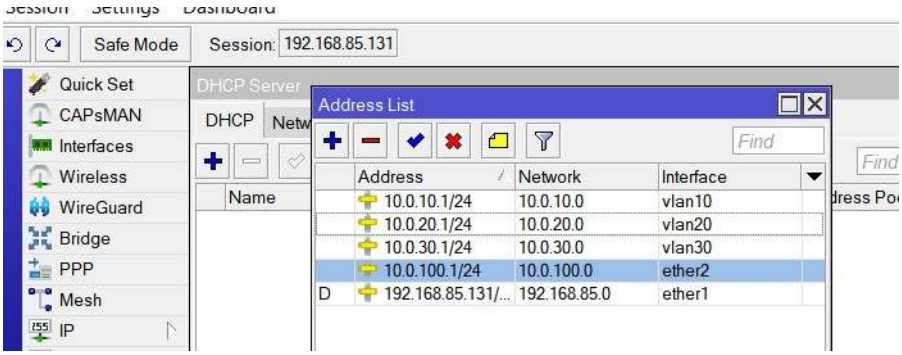
```
[admin@MikroTik] > /ip dhcp-server print
Columns: NAME, INTERFACE, ADDRESS-POOL, LEASE-TIME
# NAME   INTERFACE  ADDRESS-POOL  LEASE-TIME
0 dhcp1  vlan10     dhcp_pool0    30m
1 dhcp2  vlan20     dhcp_pool1    30m
2 dhcp3  vlan30     dhcp_pool2    30m
[admin@MikroTik] > /ip dhcp-server lease print

[admin@MikroTik] > /ip dhcp-server network print
Columns: ADDRESS, GATEWAY, DNS-SERVER
# ADDRESS        GATEWAY    DNS-SERVER
0 10.0.10.0/24   10.0.10.1  8.8.8.8
1 10.0.20.0/24   10.0.20.1  8.8.8.8
2 10.0.30.0/24   10.0.30.1  8.8.8.8
```

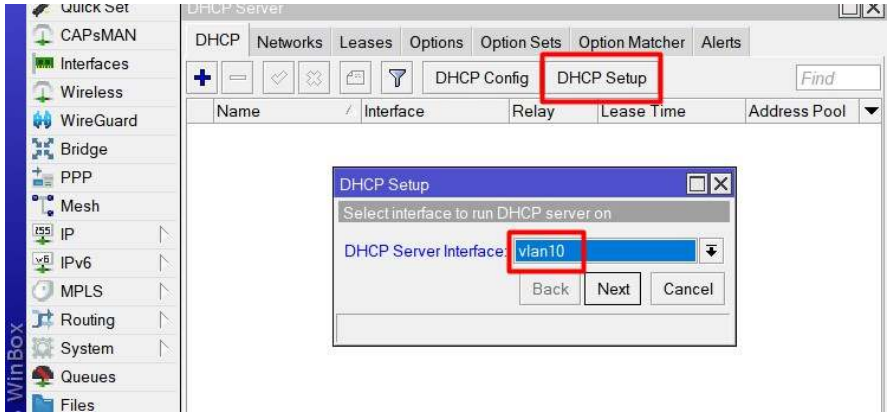
**Via Winbox:**

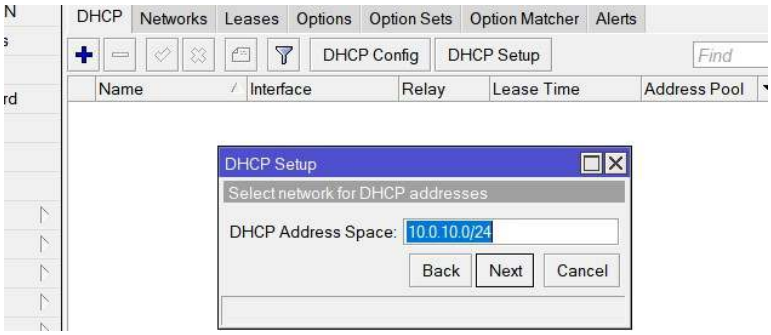



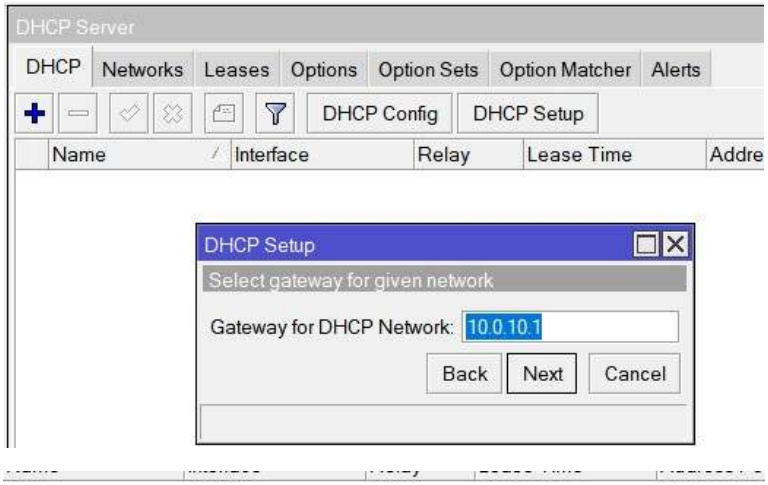



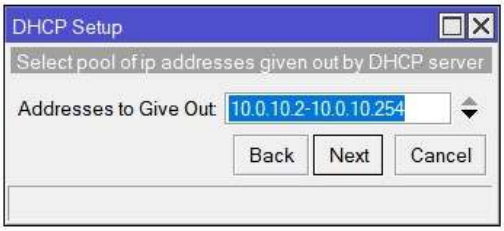

Address
Network
Interface
10.0.10.1/24
10.0.10.0
vlan10
10.0.20.1/24
10.0.20.0
vlan20
10.0.100.1/24
10.0.100.0
ether2
New Address
Address: 10.0.30.1/24
Network:
Interface: vlan30
OK
Cancel
Apply
Disable
Comment


Safe Mode
Session: 192.168.85.131
Quick Set
CAPsMAN
Interfaces
Wireless
WireGuard
Bridge
PPP
Mesh
IP
DHCP Server
DHCP
Address List
Address
Network
Interface
10.0.10.1/24
10.0.10.0
vlan10
10.0.20.1/24
10.0.20.0
vlan20
10.0.30.1/24
10.0.30.0
vlan30
10.0.100.1/24
10.0.100.0
ether2
D
192.168.85.131/...
192.168.85.0
ether1


CAPsMAN
Interfaces
Wireless
WireGuard
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
WinBox
DHCP
Networks
Leases
Options
Option Sets
Option Matcher
Alerts
DHCP Config
DHCP Setup
Name
Interface
Relay
Lease Time
Address Pool
DHCP Setup
Select interface to run DHCP server on
DHCP Server Interface: vlan10
Back
Next
Cancel

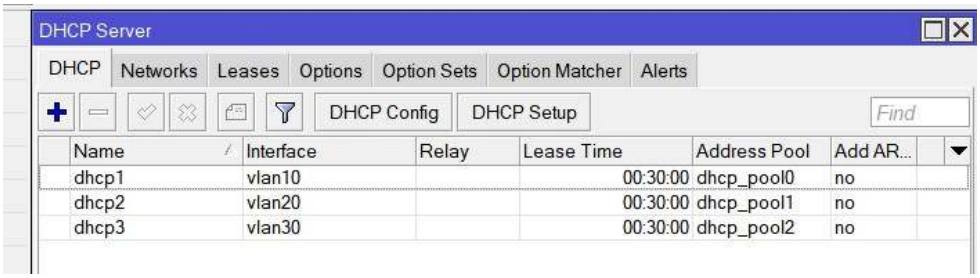

DHCP
Networks
Leases
Options
Option Sets
Option Matcher
Alerts
DHCP Config
DHCP Setup
Name
Interface
Relay
Lease Time
Address Pool
DHCP Setup
Select network for DHCP addresses
DHCP Address Space: 10.0.10.0/24
Back
Next
Cancel

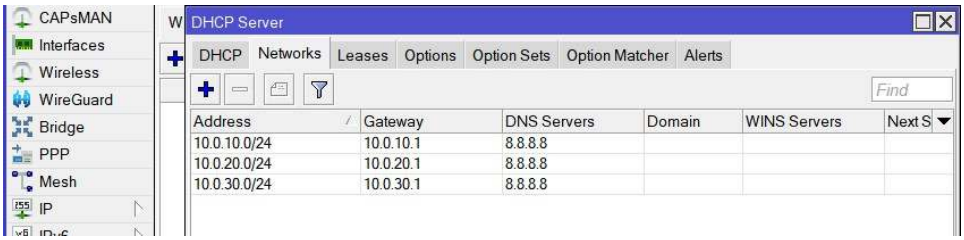

DHCP Server
DHCP
Networks
Leases
Options
Option Sets
Option Matcher
Alerts
DHCP Config
DHCP Setup
Name
Interface
Relay
Lease Time
Addre
DHCP Setup
Select gateway for given network
Gateway for DHCP Network:
10.0.10.1
Back
Next
Cancel


DHCP Setup
Select pool of ip addresses given out by DHCP server
Addresses to Give Out:
10.0.10.2-10.0.10.254
Back
Next
Cancel


Name
Interface
Relay
Lease Time
Address


DHCP Setup
Select DNS servers
DNS Servers:
8.8.8.8
Back
Next
Cancel


DHCP Server
DHCP
Networks
Leases
Options
Option Sets
Option Matcher
Alerts
DHCP Config
DHCP Setup
Find
Name
Interface
Relay
Lease Time
Address Pool
Add AR...
dhcp1
vlan10
00:30:00
dhcp_pool0
no
dhcp2
vlan20
00:30:00
dhcp_pool1
no
dhcp3
vlan30
00:30:00
dhcp_pool2
no

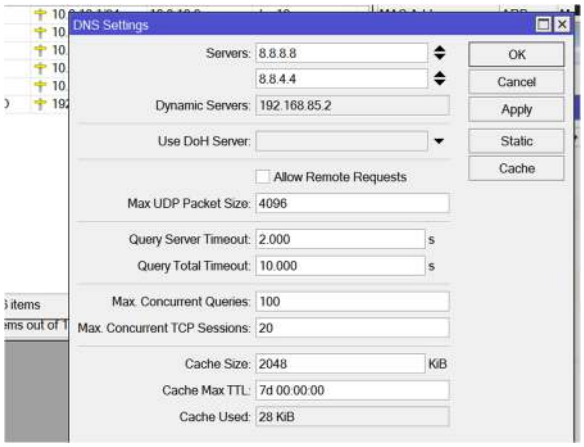



**Configuring the DNS Server settings:**

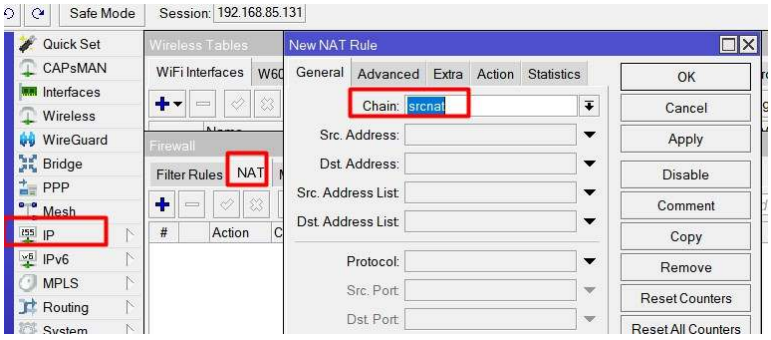
*# ip dns set servers=8.8.8.8,8.8.4.4*

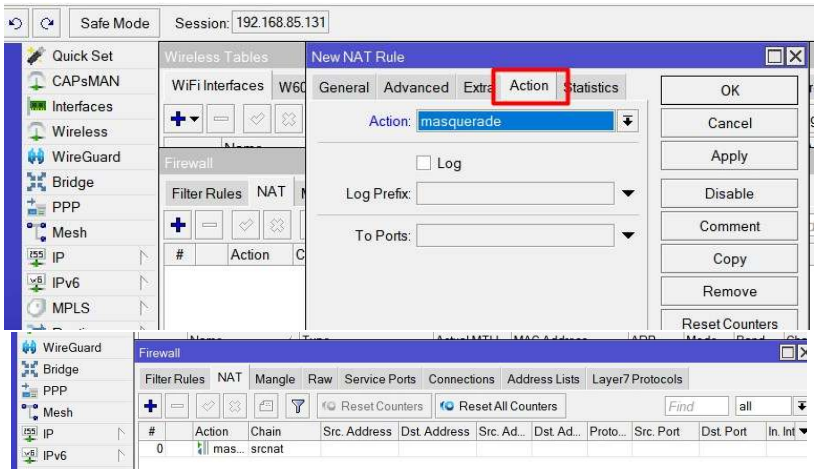
```
[admin@MikroTik] > ip dns set servers=8.8.8.8,8.8.4.4
[admin@MikroTik] > ping cisco.com
  SEQ HOST                                     SIZE TTL TIME       STATUS
    0 72.163.4.185                               56 128 54ms648us
    1 72.163.4.185                               56 128 63ms888us
    2 72.163.4.185                               56 128 56ms83us
    3 72.163.4.185                               56 128 55ms665us
    4 72.163.4.185                               56 128 54ms600us
    sent=5 received=5 packet-loss=0% min-rtt=54ms600us avg-rtt=56ms976us max-rtt=63ms888us

[admin@MikroTik] >
```

- **Winbox: IP > DNS**

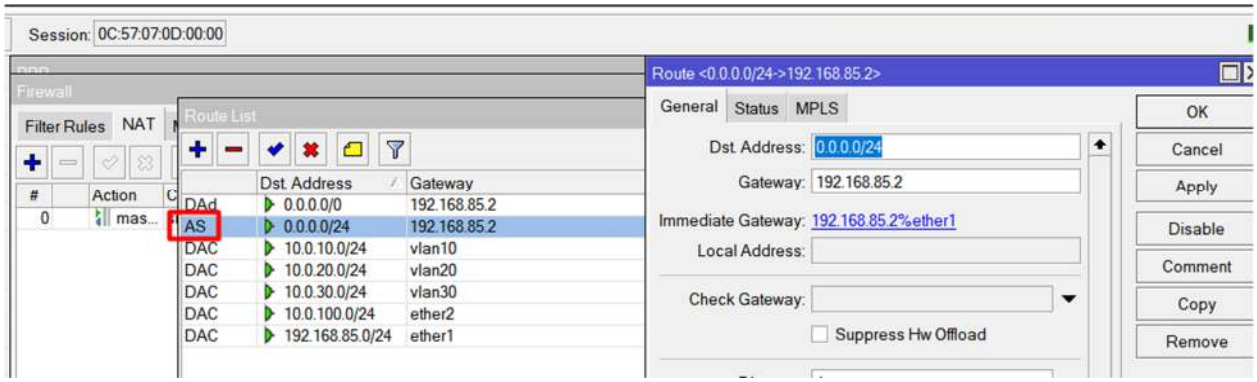



- **Firewall Setting (needs to be done to make sure users can get internet connection properly).**






**IP Routing**: Add default gateway statically, although added dynamically we need to add it manually.



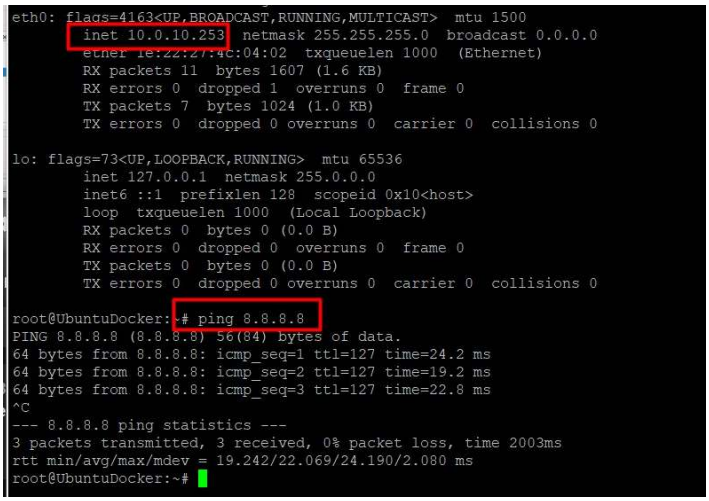

- **Interface configuration on the Docker Ubuntu (as Client).**

  To enable DHCP on the interface of the Ubuntu Docker added to your topology, right-click on the Docker instance and select "Edit Config." Then, configure the following fields accordingly.

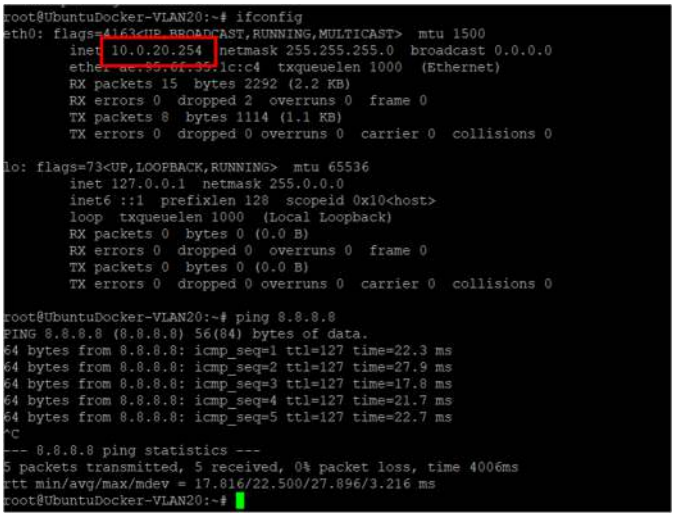
```
# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*

# Static config for eth0
#auto eth0
#iface eth0 inet static
#               address 10.0.0.25
#               netmask 255.255.255.0
#               gateway 10.0.0.10
#               up echo nameserver 8.8.8.8 > /etc/resolv.conf

# DHCP config for eth0
auto eth0
iface eth0 inet dhcp
               hostname UbuntuDocker
```

- Verify the DHCP clients can achieve the right IP from the IP Pool for each VLAN.
- Internet connectivity and DNS resolution on the DHCP Clients.

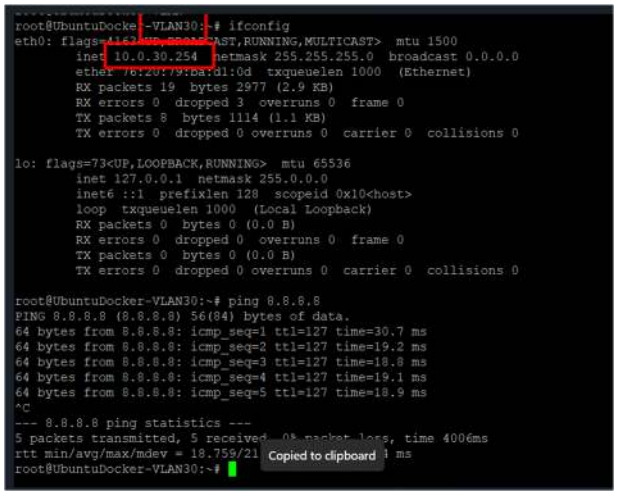
**Device in VLAN 10 >**




**Device in VLAN 20.**

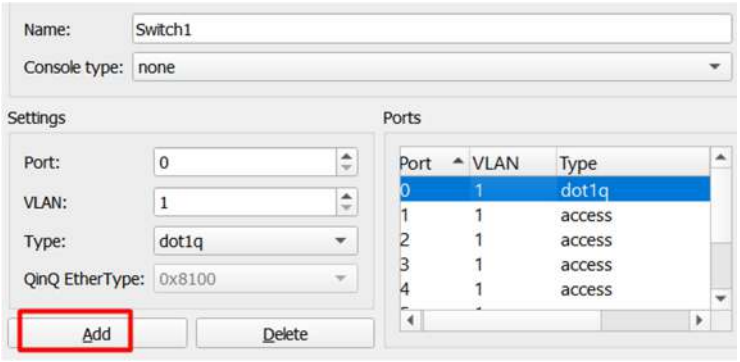



**Device in VLAN 30 >**

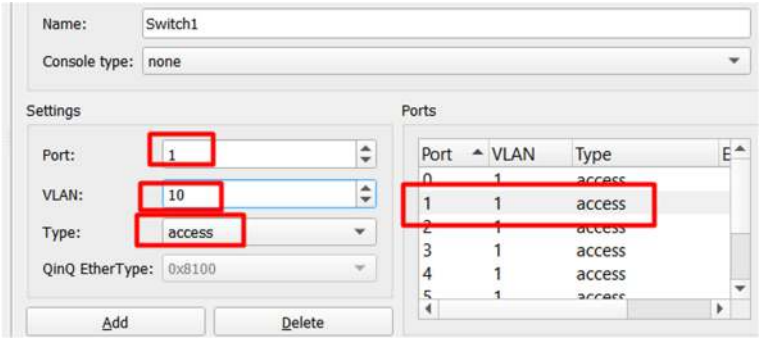


**Set up switch ports (Access port & Trunk Port).**

Interface facing the Router > Trunk port (dot.1q) : Port 0
Interface facing the VLAN members > Access port : Port 1 – 3 – 5 ( in current topology)




- **Port 1, 3 , 5 > Access Port**




As we go on more ports will be added as Access Port, via same method

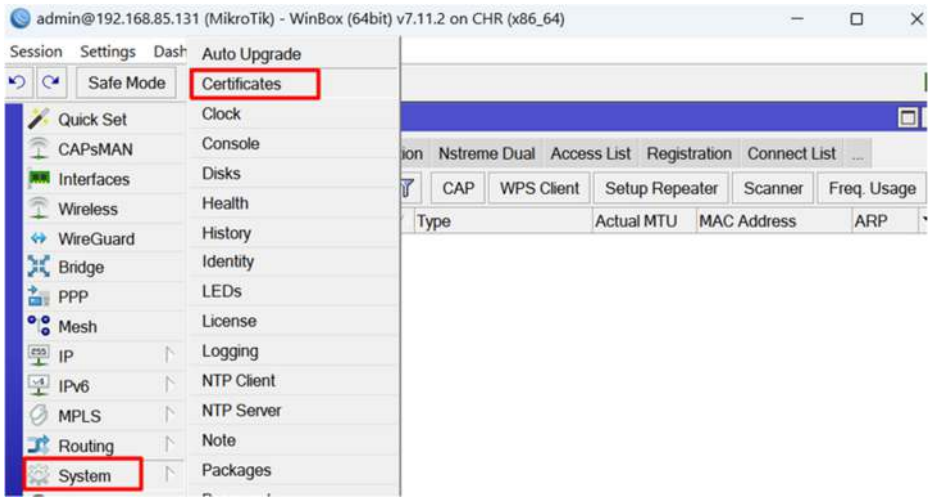
**OpenVPN Configuration:**

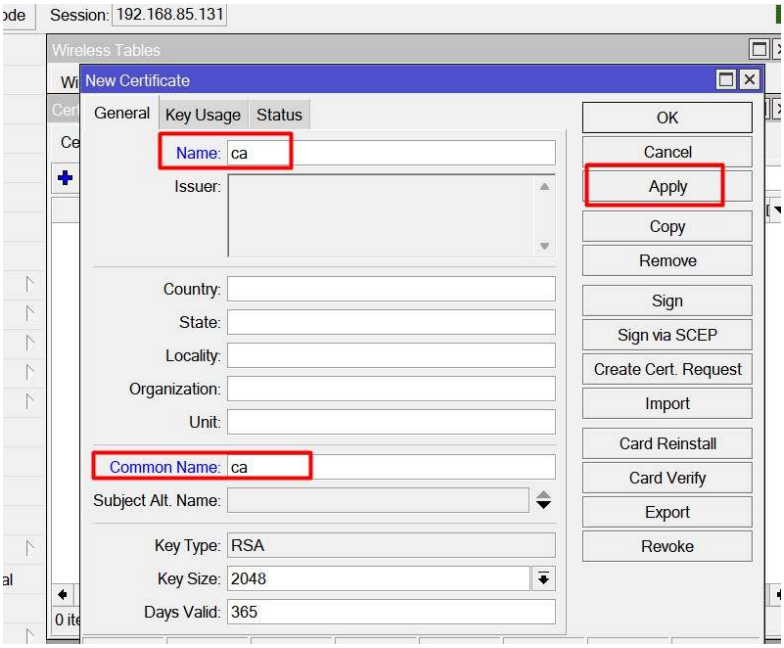
The procedure for establishing an OpenVPN connection allows a remote client (Different Network) to VPN into the VPN server (in our project, the MikroTik Router) and access the internal network behind the Firewall/Router, obtaining an IP address within the same internal network range.

OpenVPN Server and Client require three types of certificates:

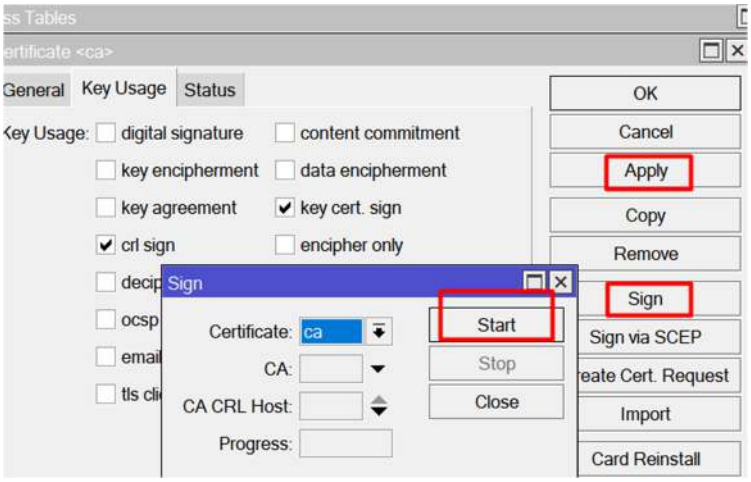
- CA (Certification Authority) Certificate
- Server Certificate and
- Client Certificate

We will start with creating the CA certificate. System> Certificates > Add + >

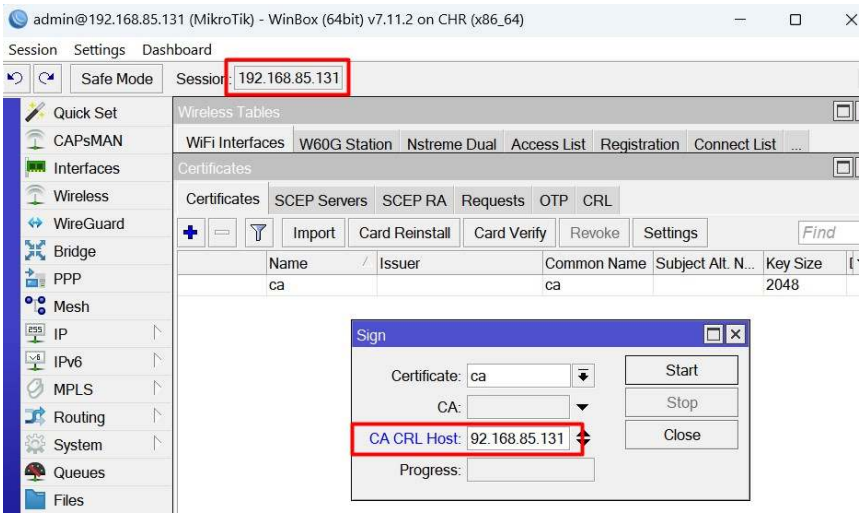

admin@192.168.85.131 (MikroTik) - WinBox (64bit) v7.11.2 on CHR (x86_64)
Session
Settings
Dash
Safe Mode
Quick Set
CAPsMAN
Interfaces
Wireless
WireGuard
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Auto Upgrade
Certificates
Clock
Console
Disks
Health
History
Identity
LEDs
License
Logging
NTP Client
NTP Server
Note
Packages
Nstreme Dual
Access List
Registration
Connect List
CAP
WPS Client
Setup Repeater
Scanner
Freq. Usage
Type
Actual MTU
MAC Address
ARP


Session: 192.168.85.131
Wireless Tables
New Certificate
General
Key Usage
Status
Name: ca
Issuer:
Country:
State:
Locality:
Organization:
Unit:
Common Name: ca
Subject Alt. Name:
Key Type: RSA
Key Size: 2048
Days Valid: 365
OK
Cancel
Apply
Copy
Remove
Sign
Sign via SCEP
Create Cert. Request
Import
Card Reinstall
Card Verify
Export
Revoke


Click on Apply the config and sign the Public Key.

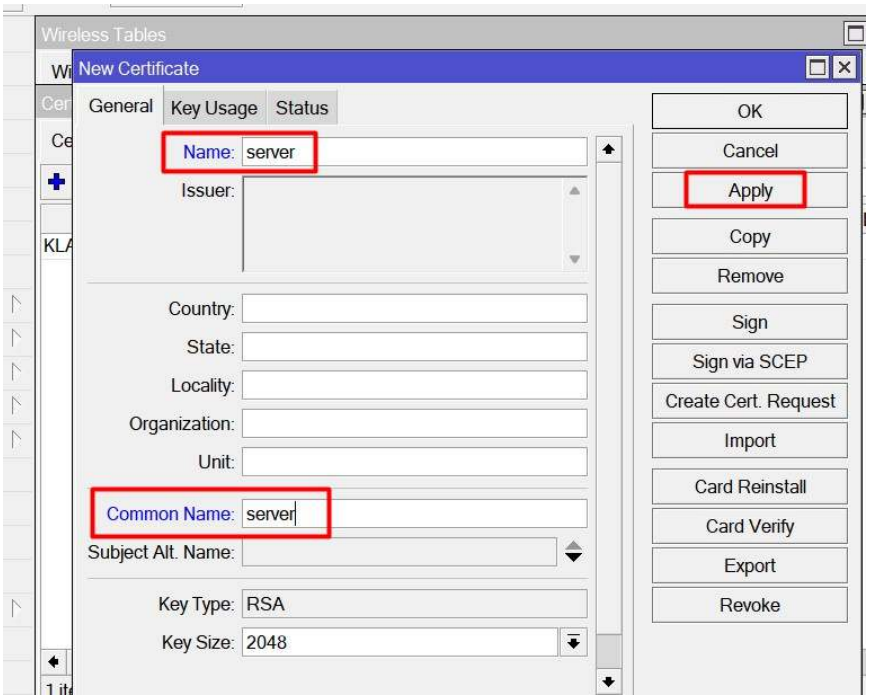



CA host is the IP Address of the VPN Server ( WAN interface of the Router).

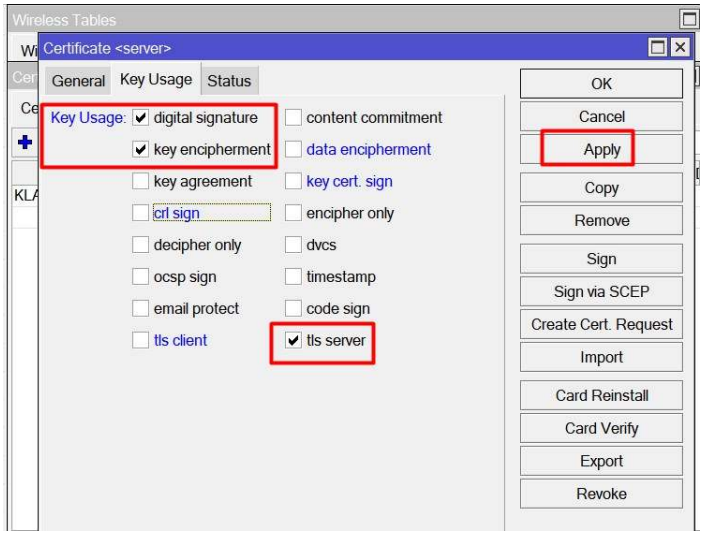


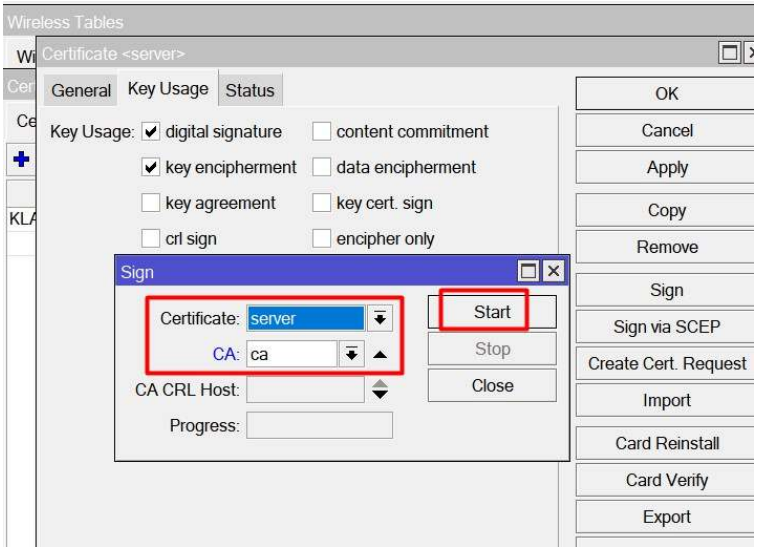

Once the certificate has been siged ( Progress Done) we can close the window.

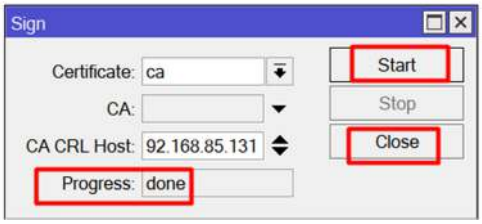

Next we will add Server Certificate. We will add another new certificate:

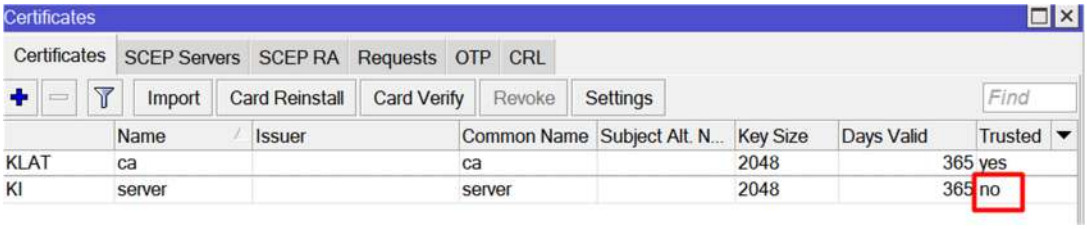


Public Keys needs to be signed.

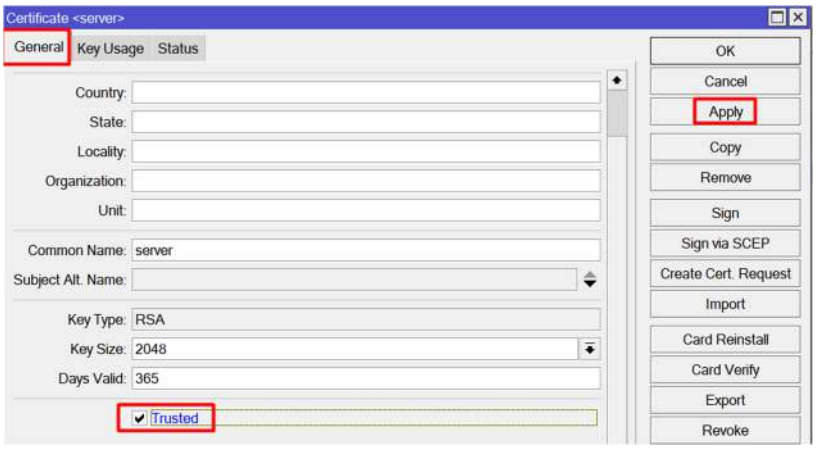


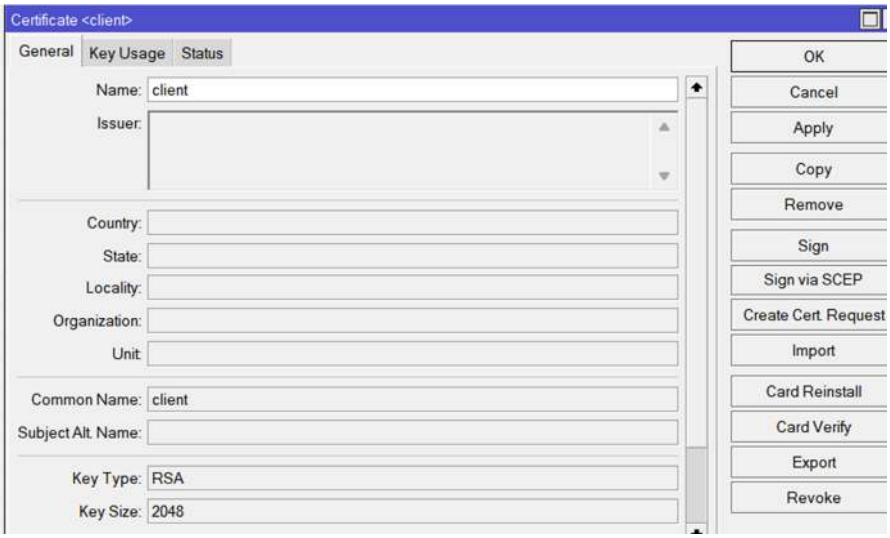



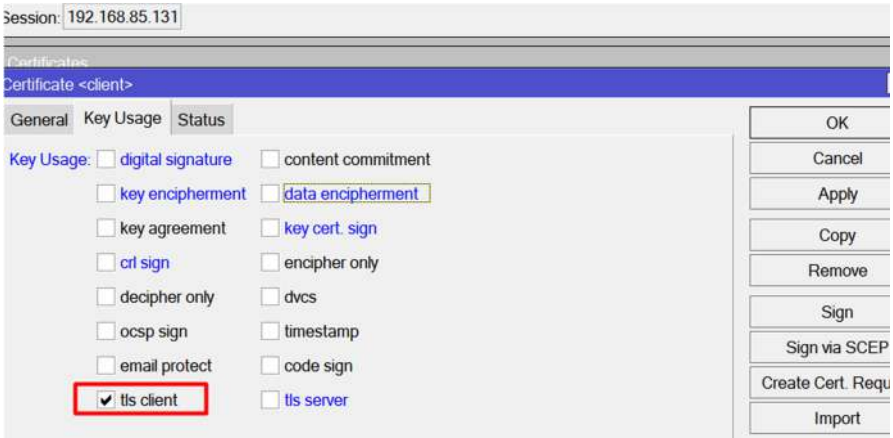



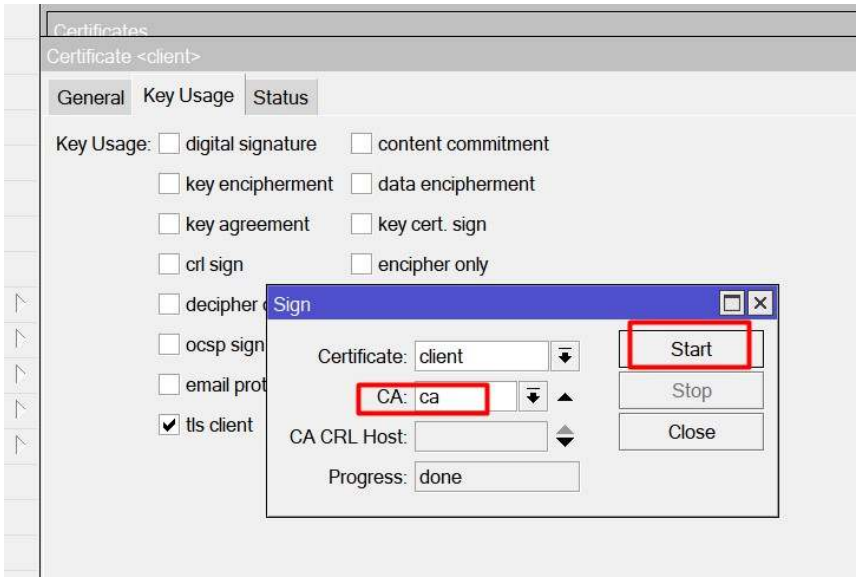
We need to make sure CA and Server certificates are Trusted. Click on the certificate and under general tab check mark the Trusted option.



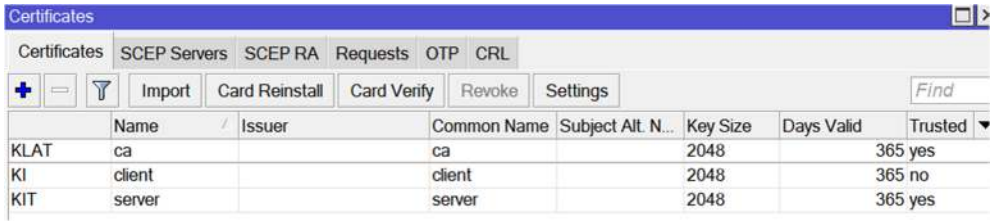

Next is time to add Client Certificates:



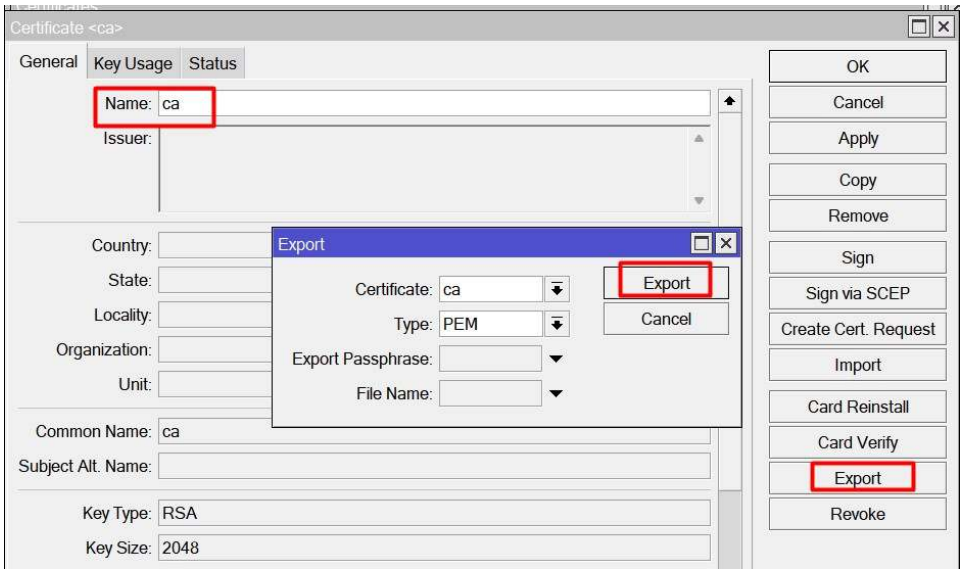



All three certificates has been added.

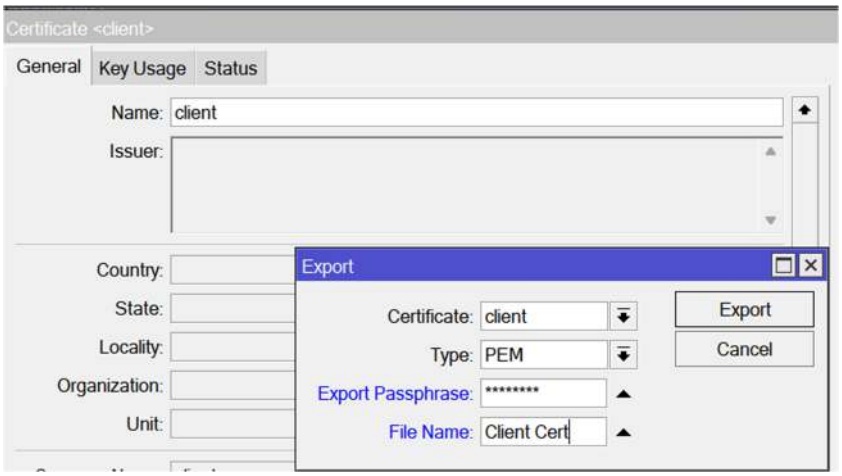



Next step: Exporting the CA and Client Certificate, Once you Export the cliet certificate it ’ll also generate a key along with it. The certificate needs to be provided to the VPN client.

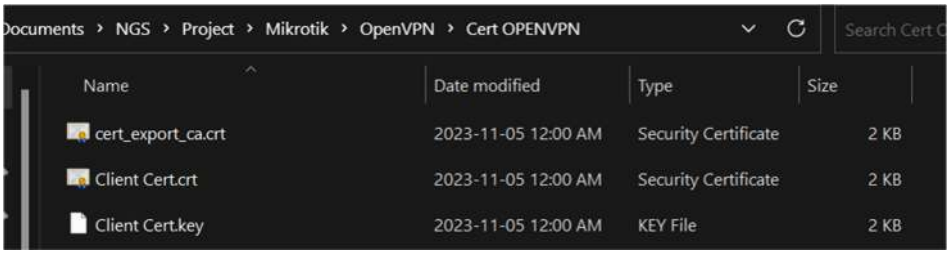
We need to click on CA and Client certificates , open it and export them.

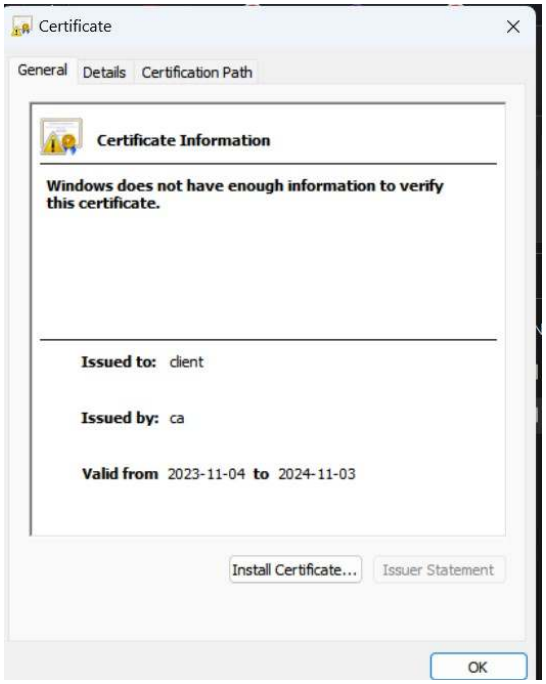


You'll be prompted to set up a password, and you do need this password during the installation of the VPN Client.

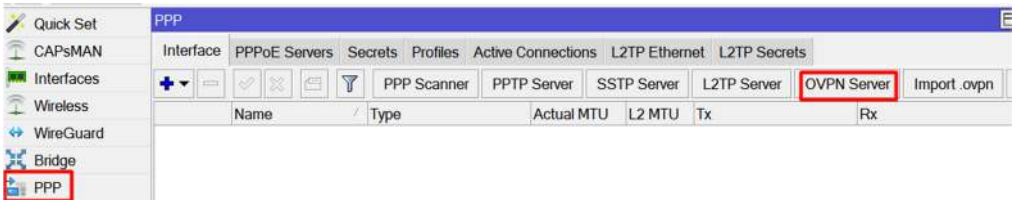


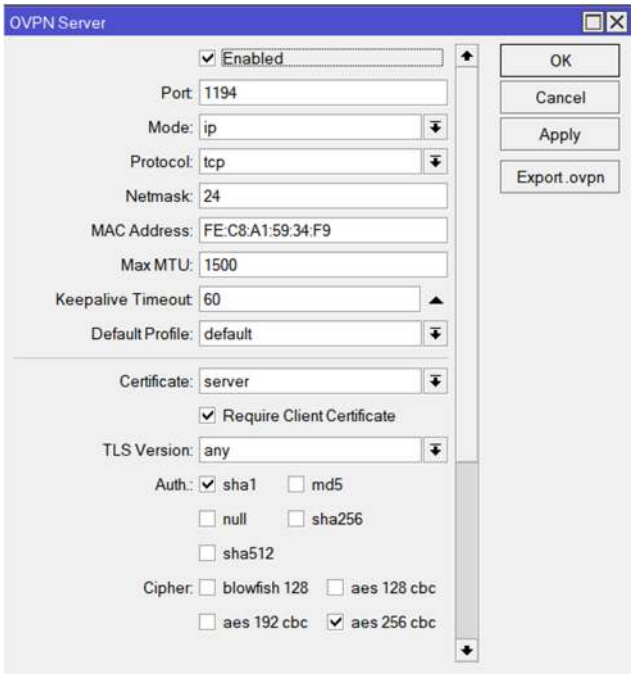

The exported certificates will be stored in the 'Files' directory. You need to copy these files to the remote system where the OpenVPN client will be installed.



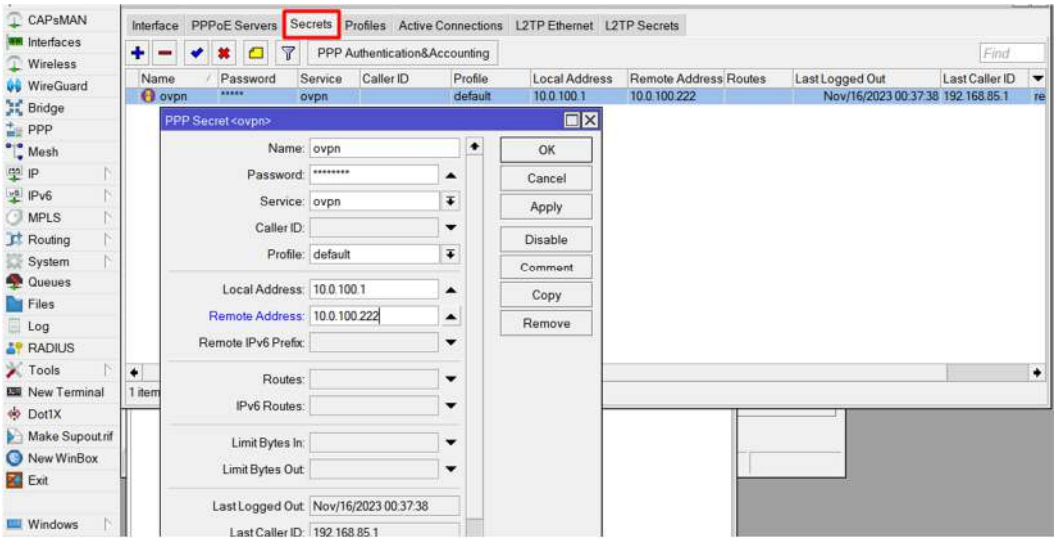



Now we do need to configure and set parameters for the OpenVPN Server on the Mikrotik Router. Configuring OpenVPN Server ports, Authentication method, Cipher..



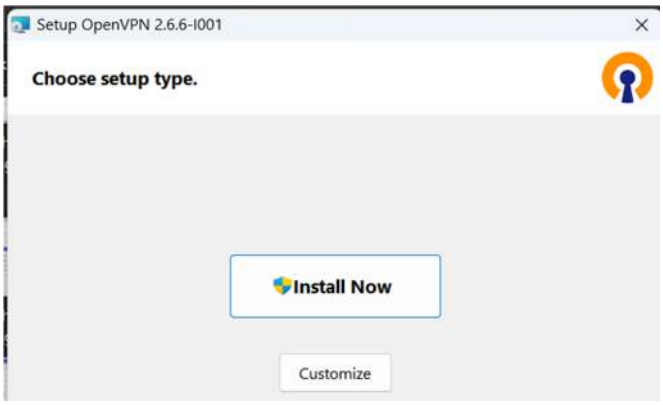

In the 'Secret' tab, configure the network address of the interface or the network to which you want the VPN client to have access. Specify the IP range (in my case, with only one VPN client, you can configure an IP pool and add it here). In my topology LAN interface IP : 10.0.100.1 (Ether1). VPN User assiged IP: 10.0.100.222



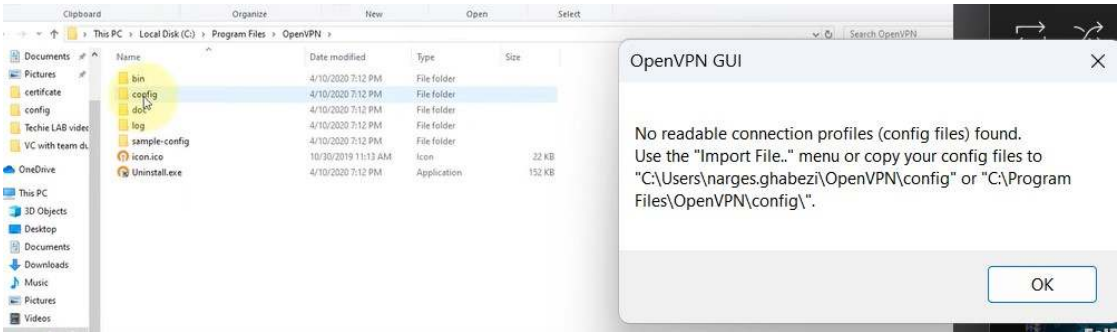
At this step we can install the VPN Client , (the host machine was a Windows System).

VPN Client can be downloaded from here, [https://openvpn.net/community-downloads/](https://openvpn.net/community-downloads/).

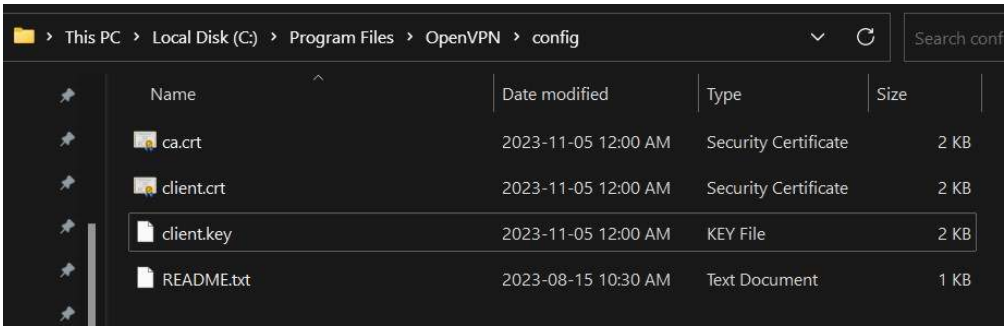
Install the Downloaded VPN Client on the VPN Client host; ( Win 10)



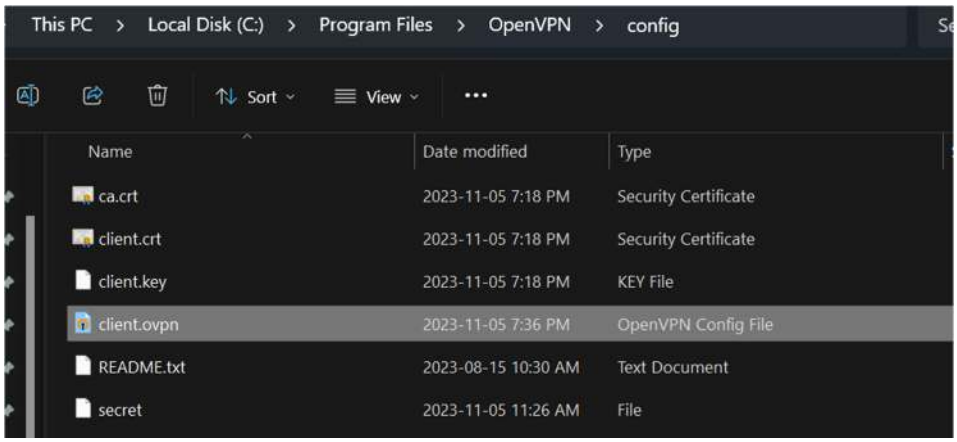

Once the VPN Client is installed you need to config the VPN Client using the certificate files you have exported, and copied to the VPN Client host.

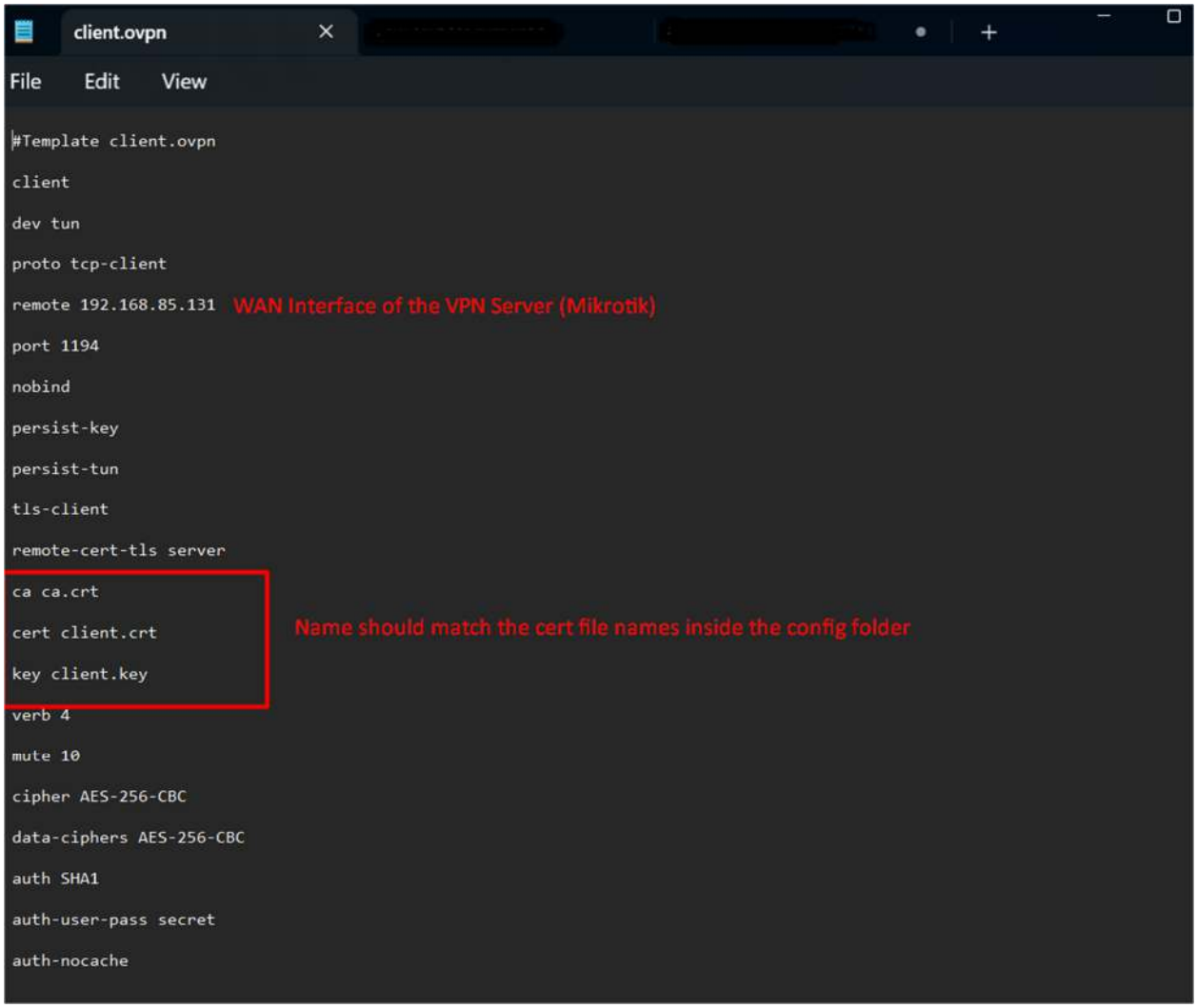



Copy to the config folder under OpenVPN installation directory, and rename them as below.

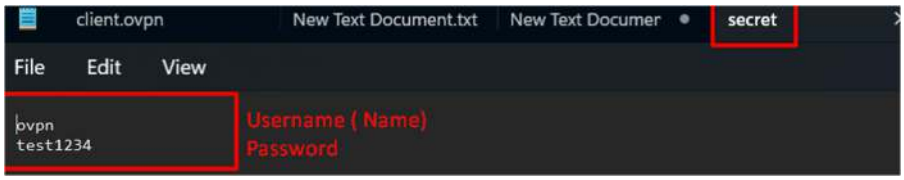


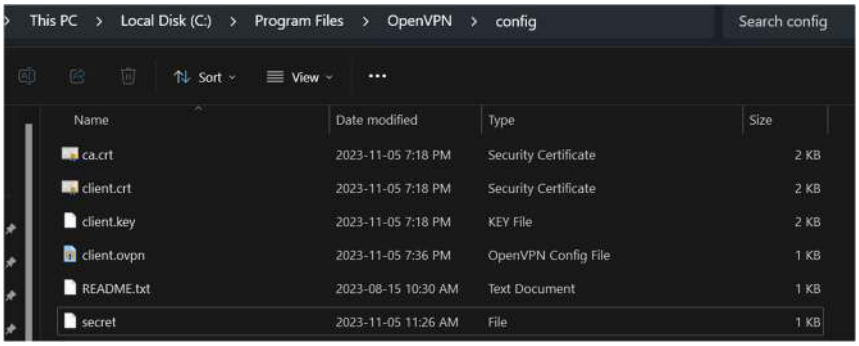
Now we need to create a text file, edit it as below and save it as .ovpn file. All the parameters should match with VPN Server configs inside the VPN Server.



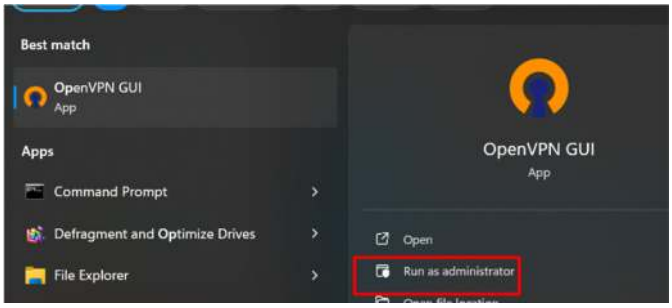



We will create another Text file, name it as secret without any extension, and Enter the user/pass you have configured under secret tab during the OpenVPN server configuration. User/pass in the secret file will be used to dial the VPN server.

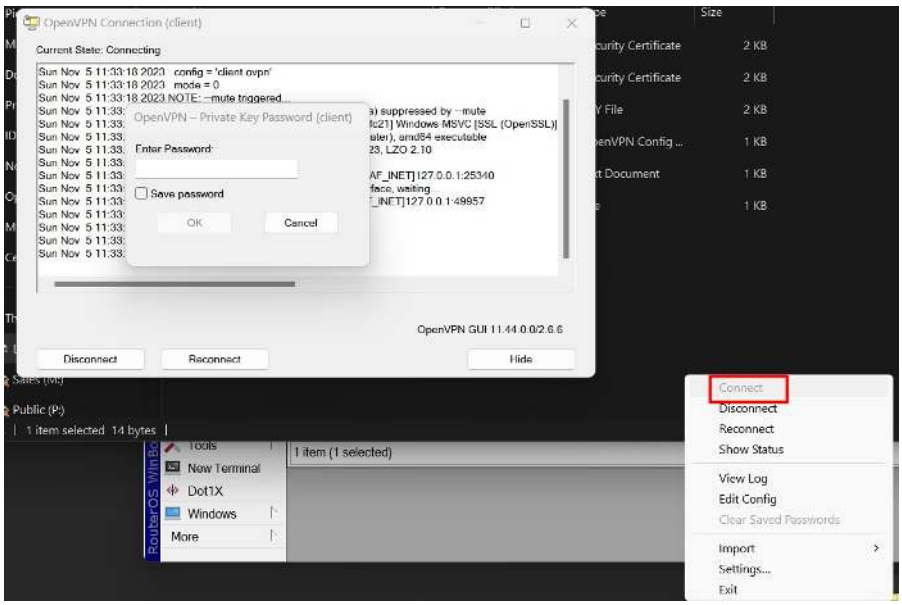


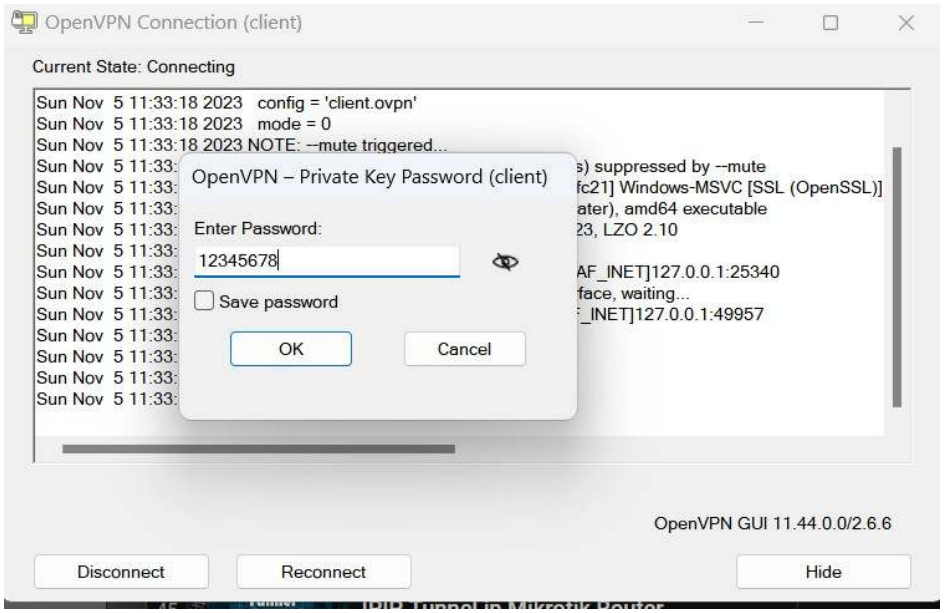




All configurations are in place; it's time to launch the VPN client.

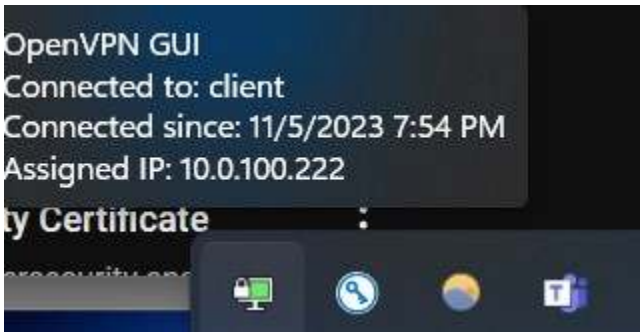








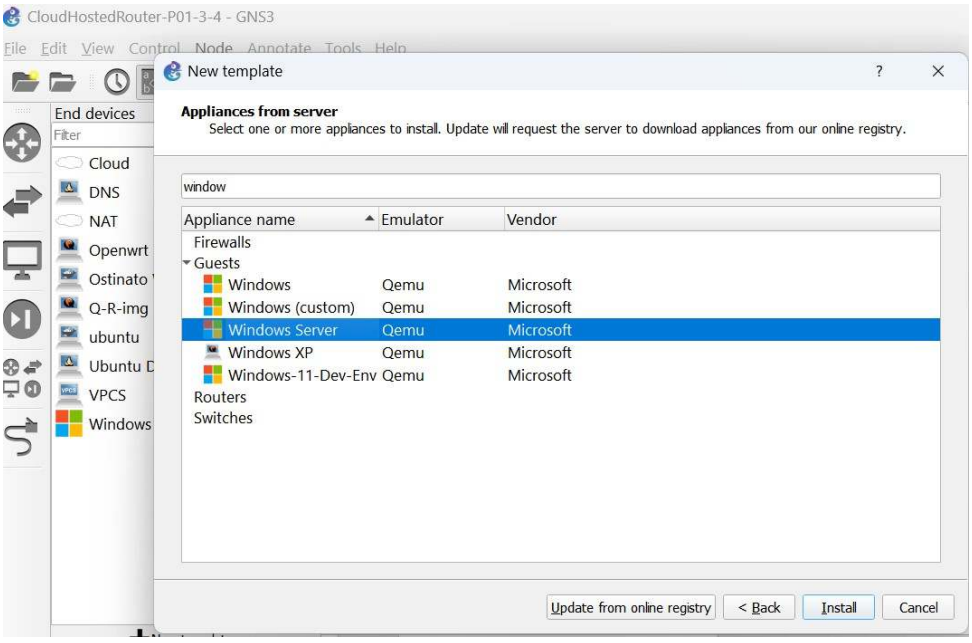

The remote system has successfully connected to the VPN server, and it has been assigned an IP within the local network range (remote machine IP).

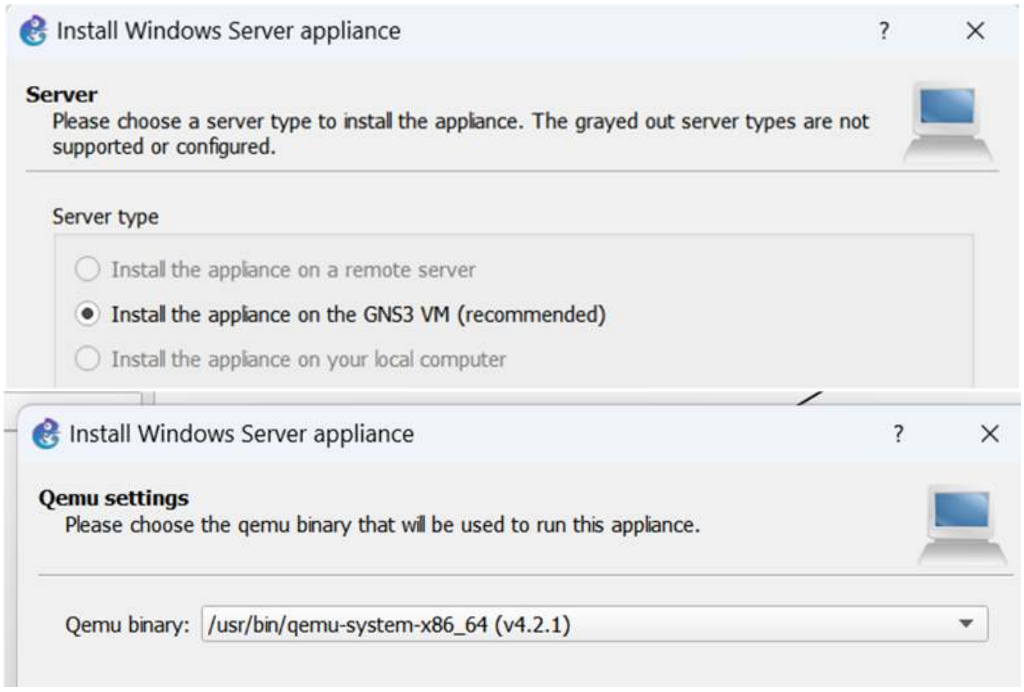


**Email Server Configuration**

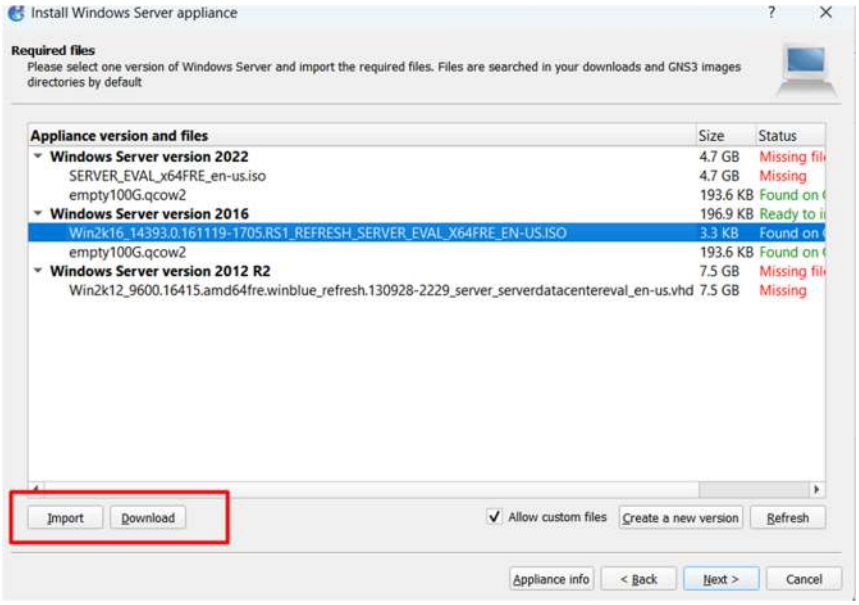
- **Installing Windows Server (as Email Server Host)**
- https://www.gns3.com/marketplace/appliances/windows-server
-


- Adding a new template and installing the Windows server

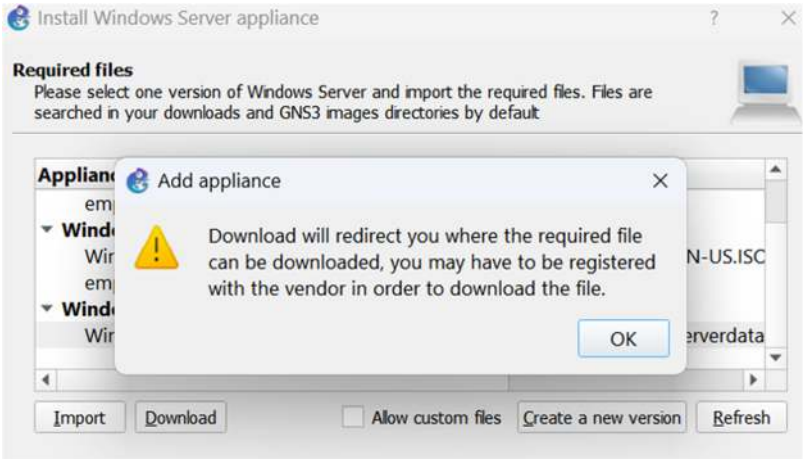




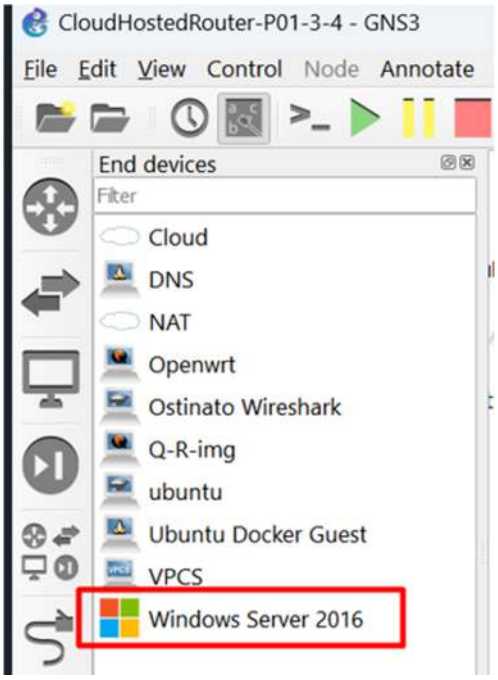

At this point, you should select the preferred Windows Server version. You have the option to download the image or import one that is already stored on your system.



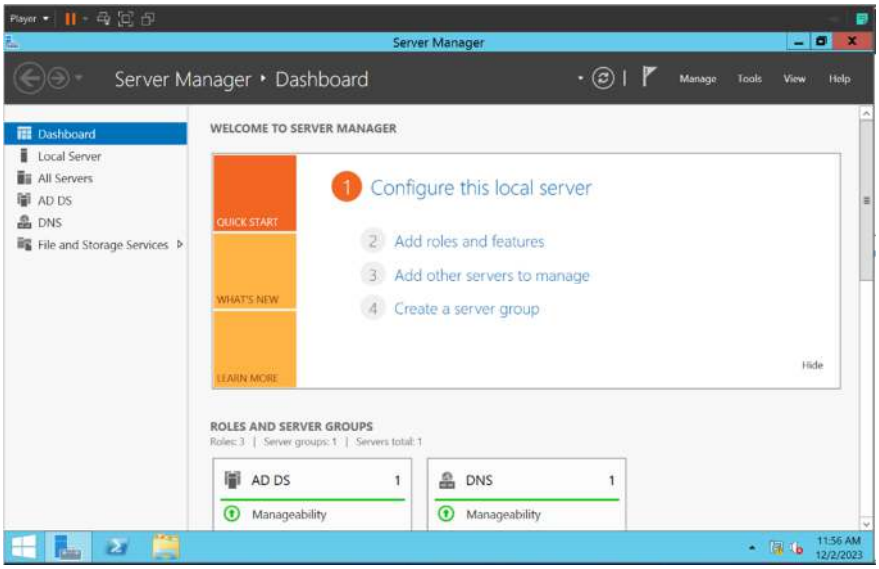
Please note that, in case of need to the download the image, by clicking on the download button you'll get redirected to website, where you file can be downloaded.



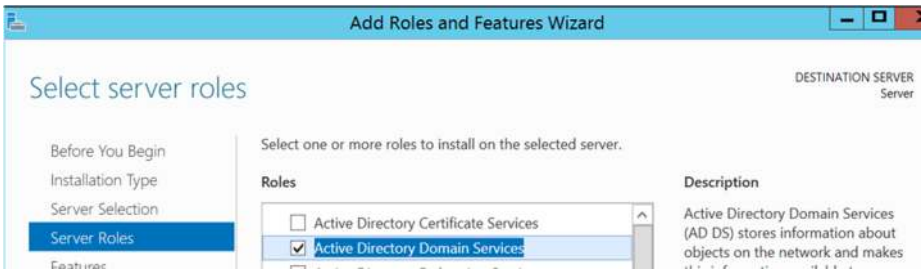

Finally, your Windows Server will be added under your devices. And can easily be added to your topology.

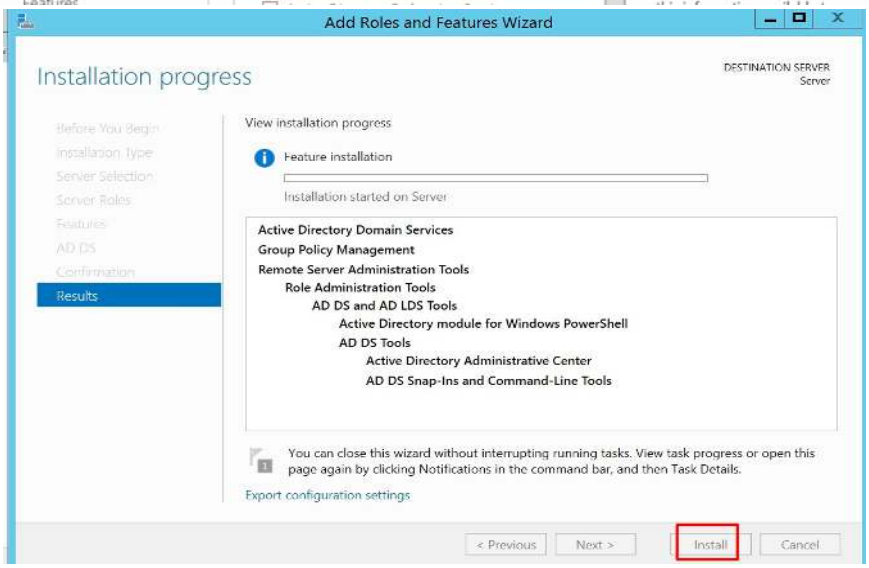


- Here your Windows Server is ready, you can add it to your topology and start the server.




- I'll initiate the setup of the Active Directory and DNS Server roles on this server. This pre-emptive step is taken to ensure that, in the later stages, the hMailserver can successfully meet all required checks for configuration and health verification( Green status). It's important to note that for installing hMailServer, Active Directory is not a mandatory requirement and may depend on your specific network topology.
-

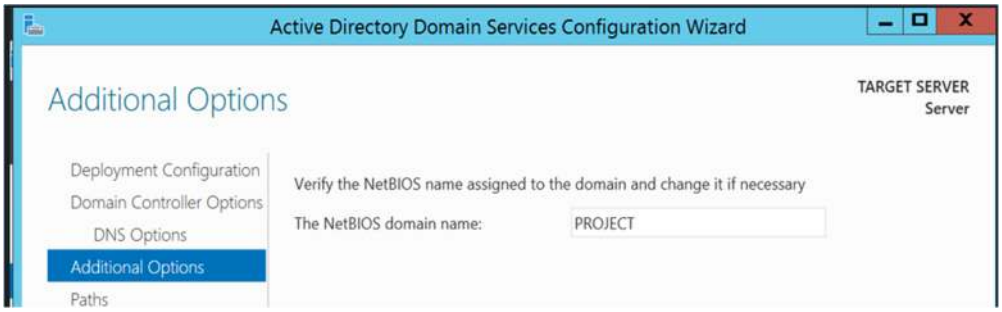


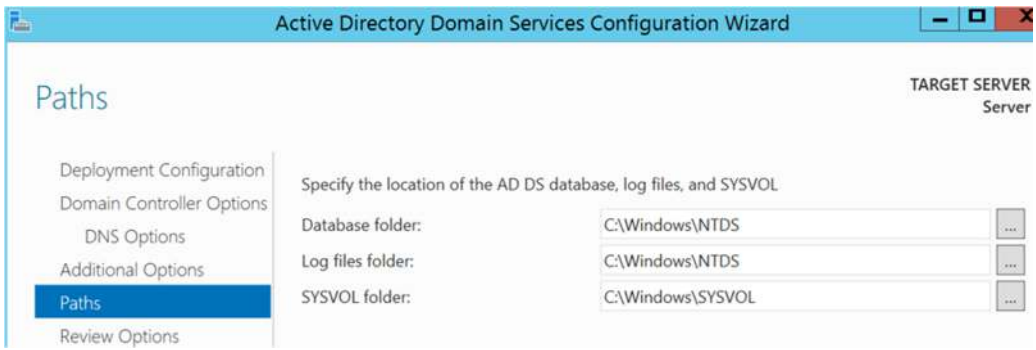
- Click on yellow tringle and promote this server to a domain controller.


- Choose the desired Domain name (which later can be used for Mail server Domain).


- Select everything as default and Next …

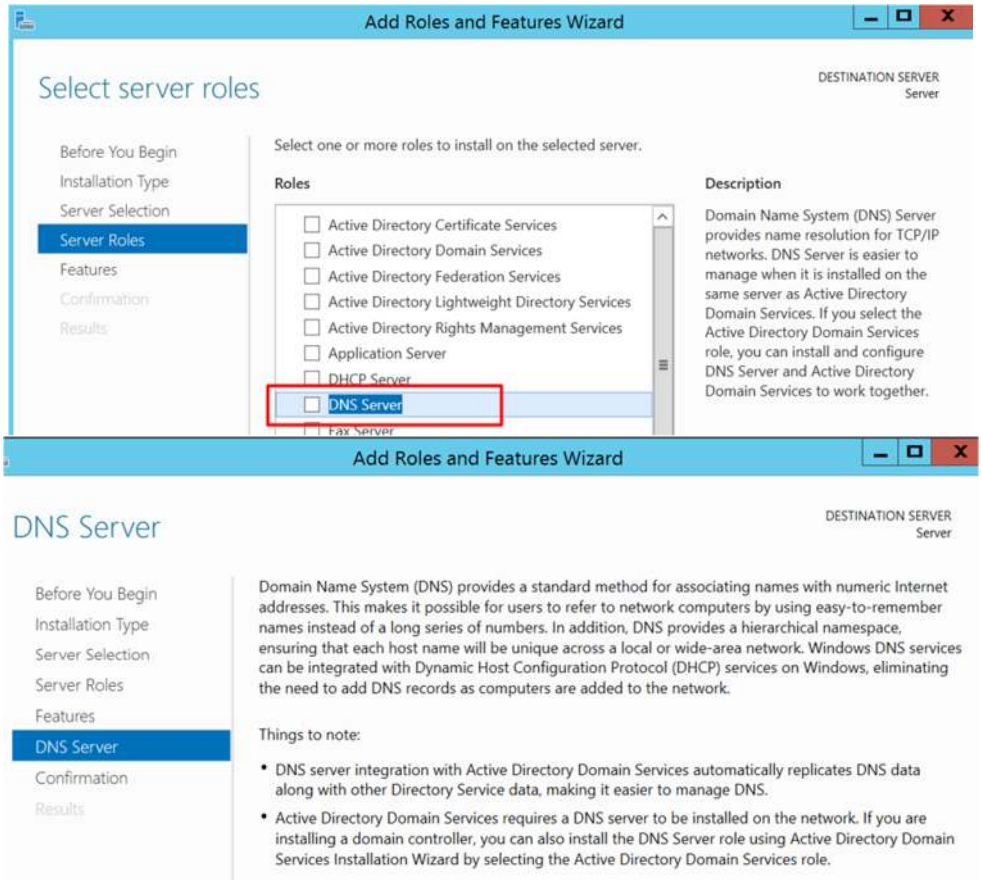



- And install >Finish. (Do <u>not modify Database directories</u>)

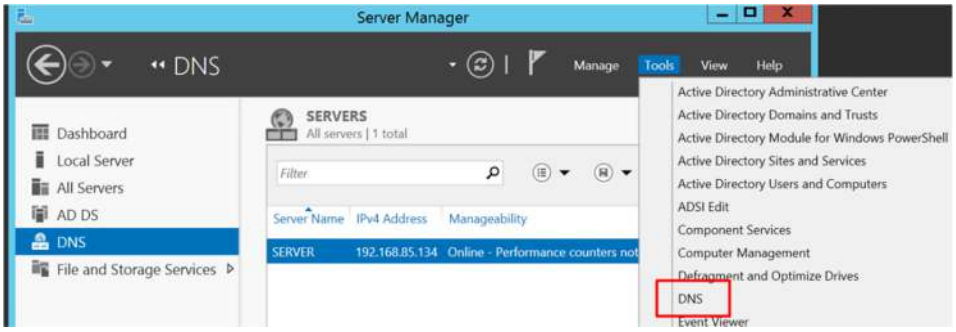


**Setting up the DNS Server:**

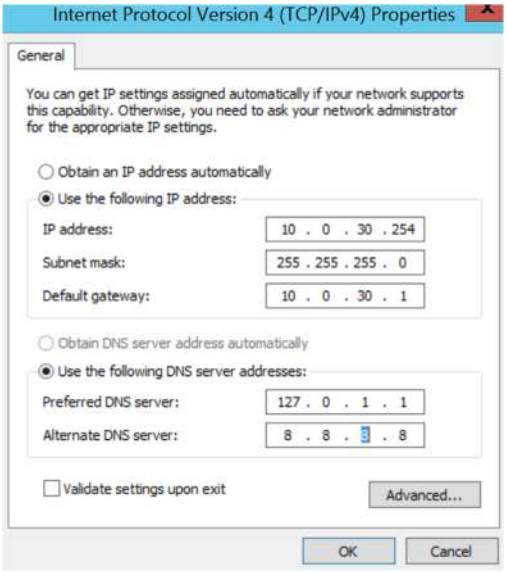
- Adding the DNS Server role:




- Once the DNS Server is installed, it will get added under the Server Manager tools. You can click on it and start configuring the DNS.




- Our MailServer belongs to VLAN 30 and is capable of receiving a DHCP-assigned IP. However, for the sake of consistency, we will set up a static IP configuration on the server.
- The primary DNS Server is set to the local host address 127.0.0.1, pointing to the server itself.



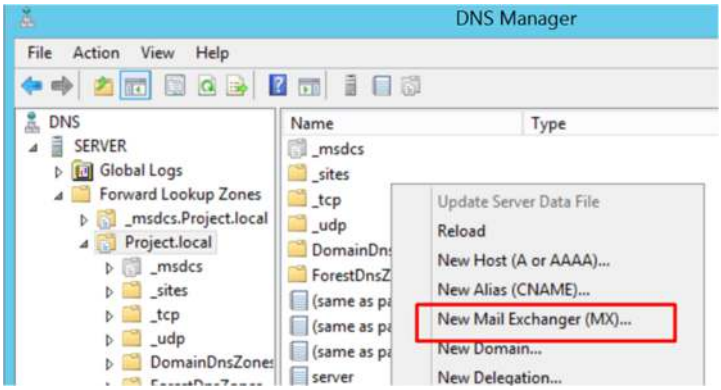

**DNS Records needs to be added:**

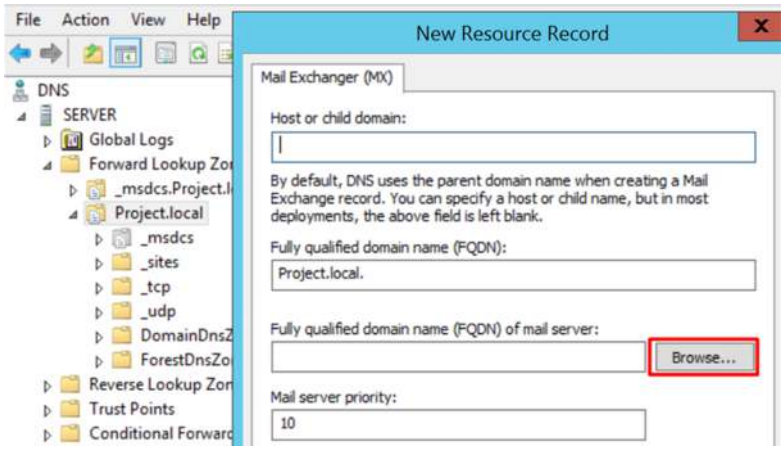
**A (Address) Record:** (by installing the DNS server A record for the server itself will be added)

- The A record maps a domain or subdomain to its corresponding IP address.
- It provides the actual IP address where the mail server can be reached.
- Example A record: mailserver.example.com. IN A 10.0.30.254

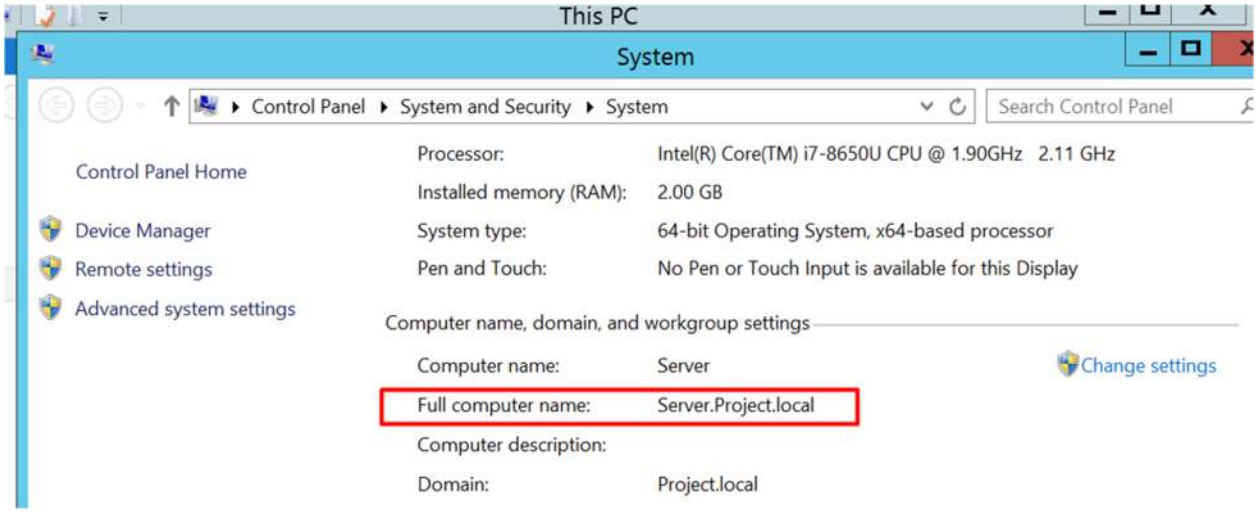
**MX (Mail Exchange) Record:**

- The MX record specifies the mail servers responsible for receiving email on behalf of a domain.
- It contains information about the mail server's hostname and its associated priority.
- Navigate to the Forward Lookup Zone: In the DNS Manager, navigate to the forward lookup zone for the specific domain where you want to add the MX record.
- Add MX Record: Right-click on the zone and select "New Mail Exchanger (MX).

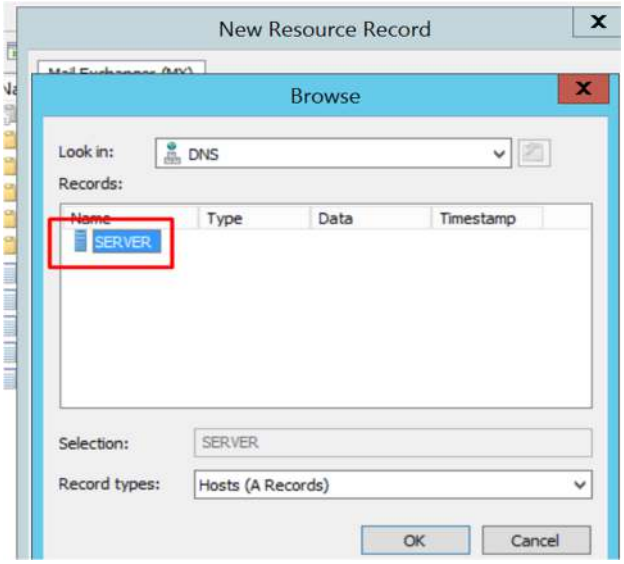


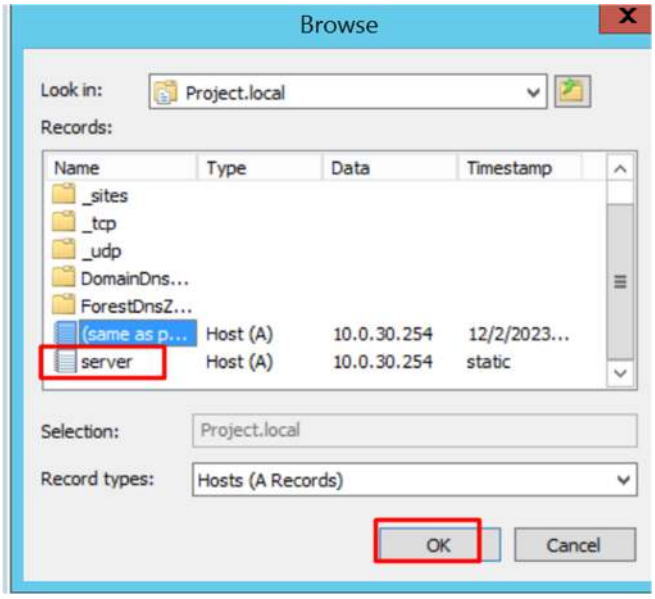


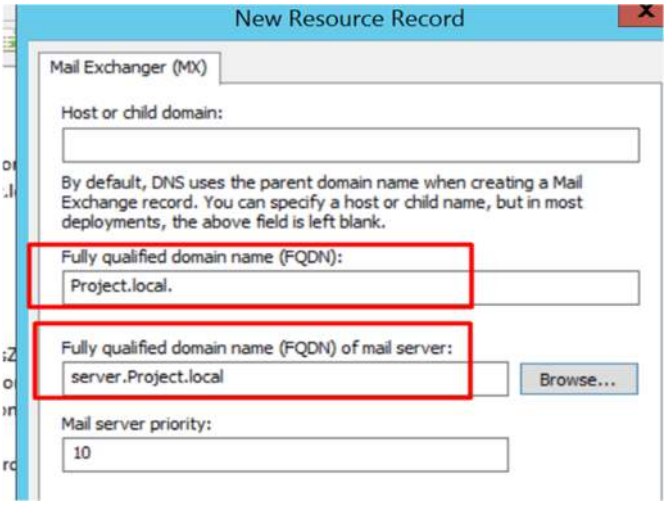

- Choose you Host Machine: (in my case the name of the host is SERVER):



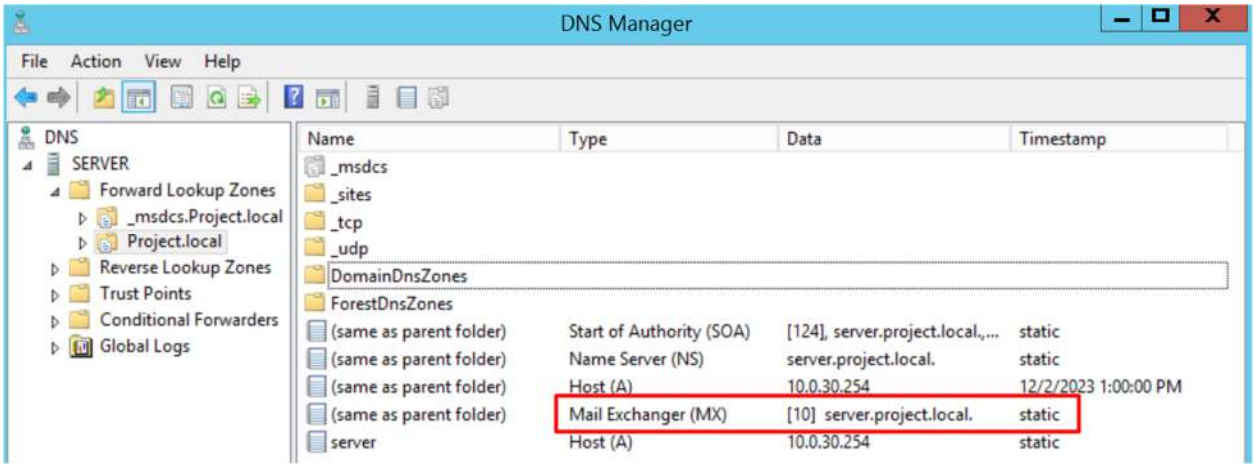

-



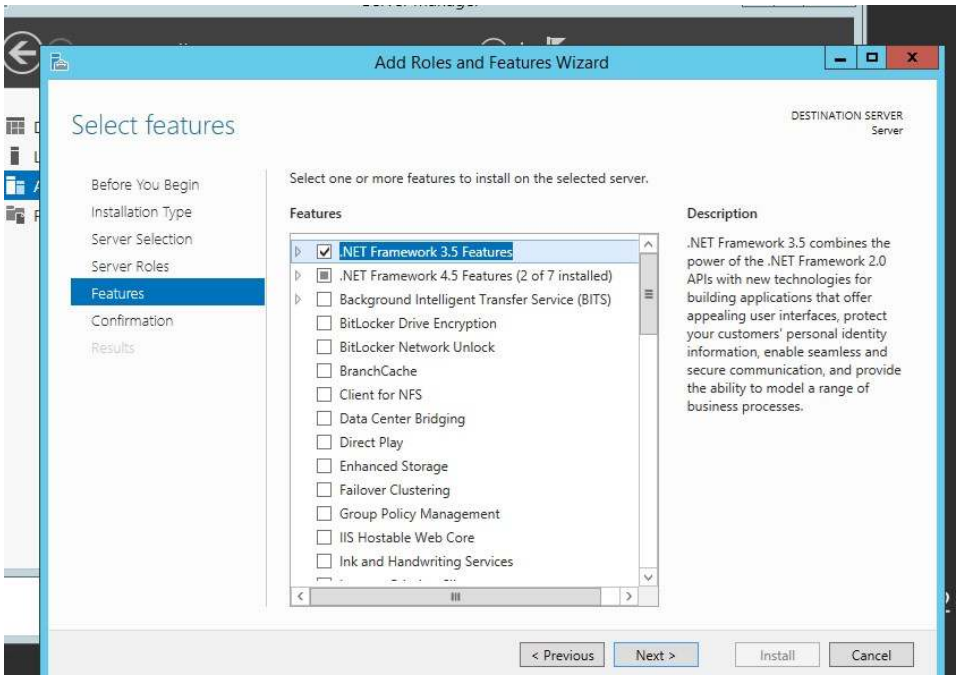



Finally, you MX record successfully has been added.



- To avoid errors during hMailServer installation, a crucial step is to install the .NET framework 3.5 feature using the "Add Roles and Features" functionality.

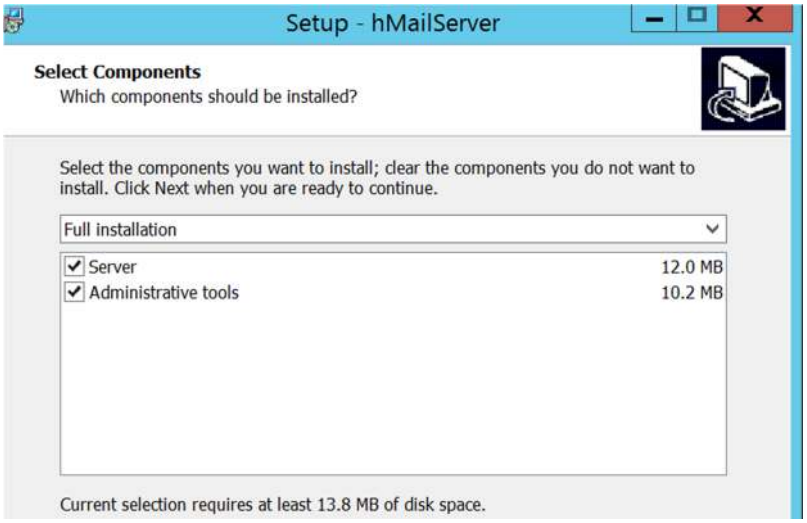


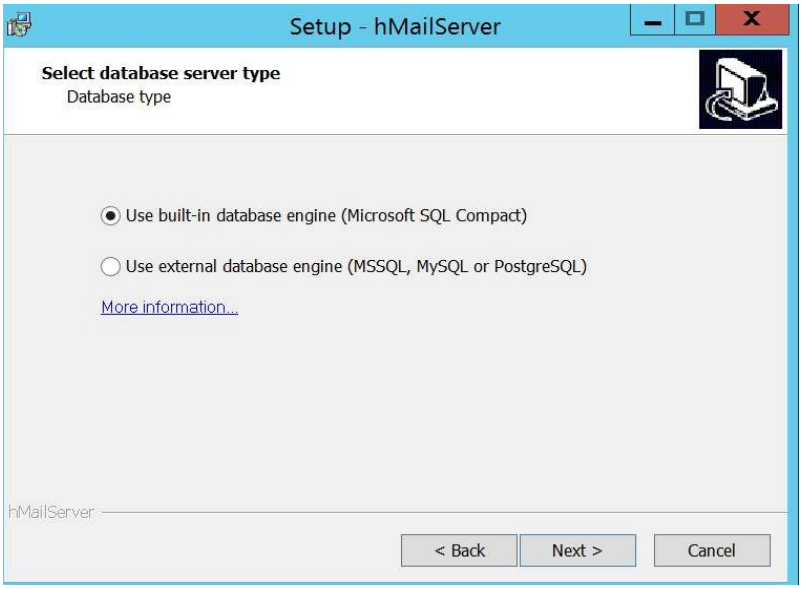

**Configuring an email server with the use of hMailServer**:

**hMailServer:** a free and open-source mail server software for Microsoft Windows. It provides email services using the standard email protocols (SMTP, IMAP, and POP3). Here are some features of hMailServer**:** Webmail, Domain and Account Management, Built-in Anti-Spam and Anti-Virus, Database Support, Rules and Filters, SSL/TLS Encryption, Logging and Monitoring, simple configuration, light weight.

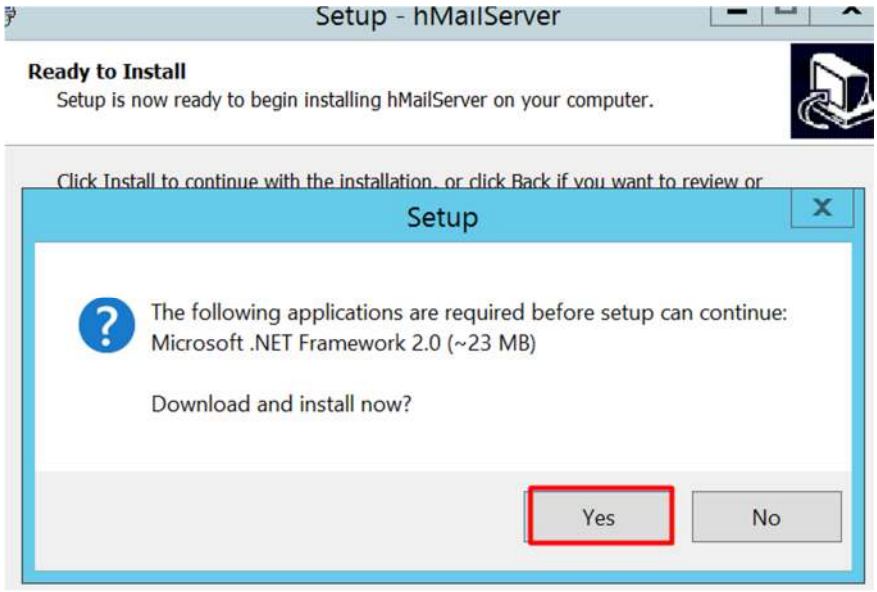
hMailServer can be downloaded from: [https://www.hmailserver.com/download](https://www.hmailserver.com/download)

- Download the hMailServer Software and run as administrator and follow steps as below.
-



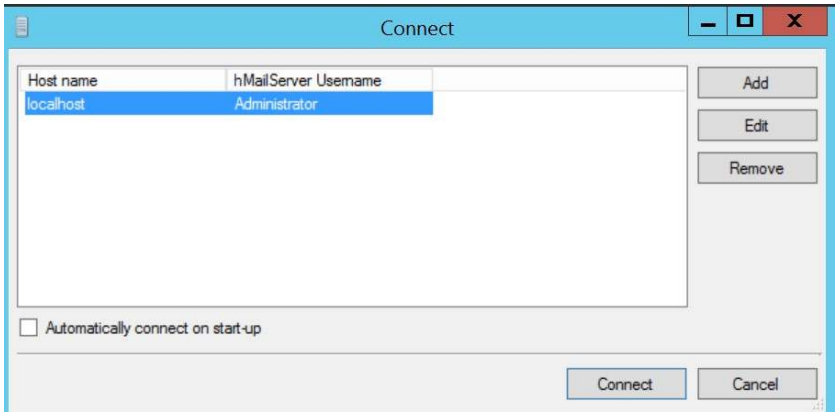

Follow choose the configs as default > Next .. > Choose a secure password.



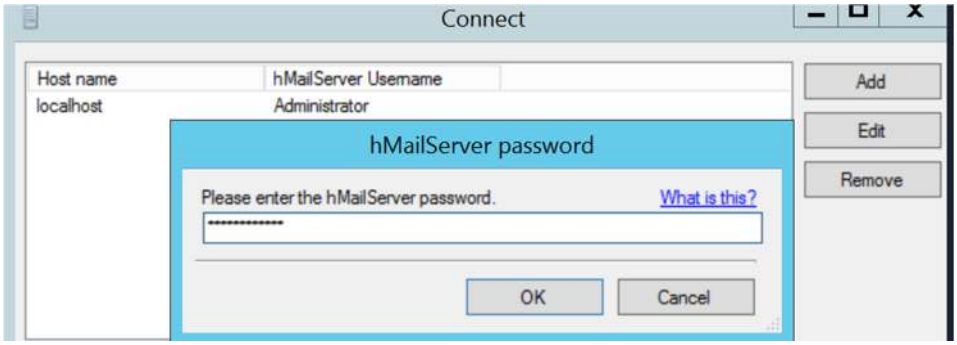

Note: If you did not already add .Net framework feature you'll face Error here.


**hMailServer configuration:**

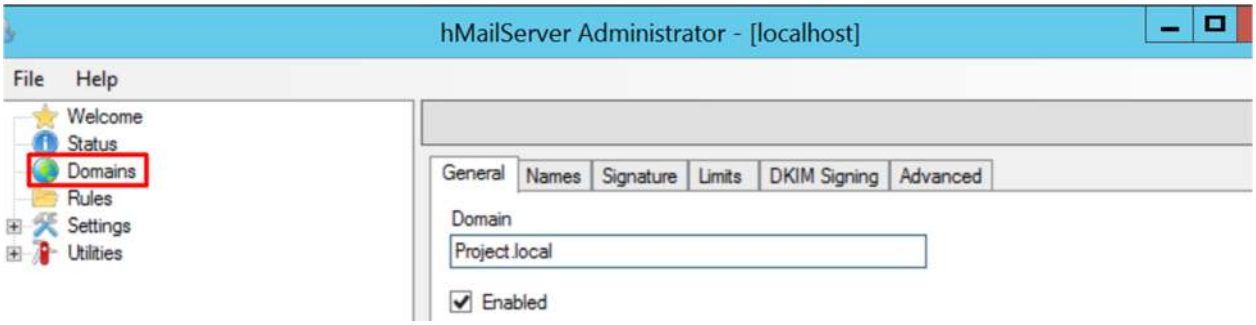
- Run the hMailServer as administrator. Connect to the server on your host machine.



- Enter the password you have set up during the installation.

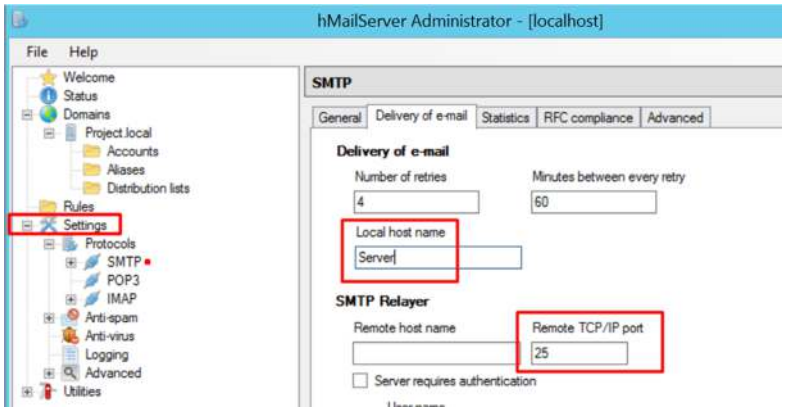



- Start by adding your domain (for Email address).

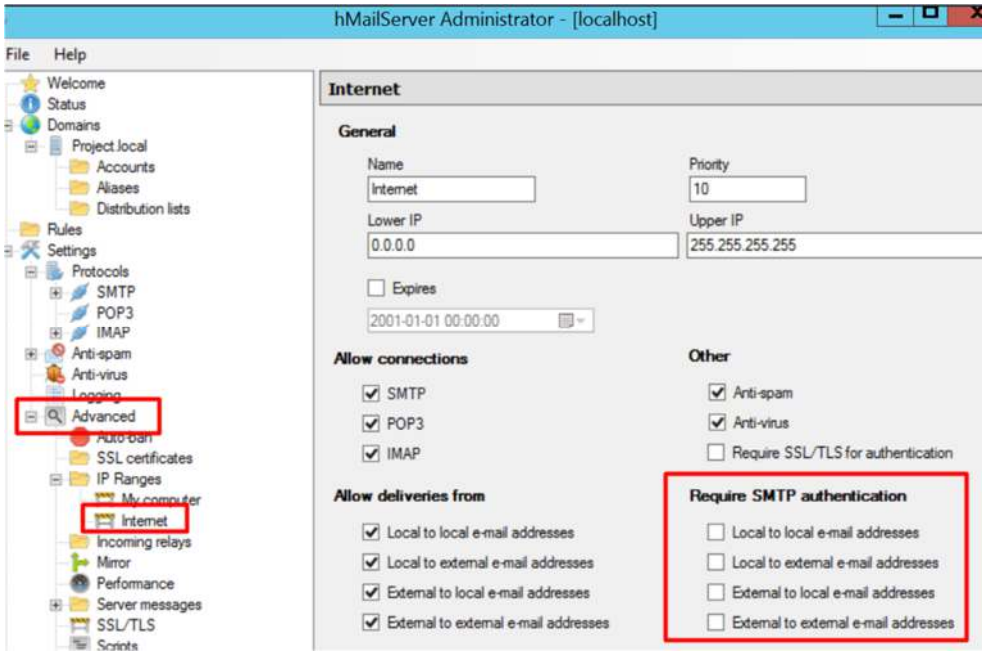



**Configure SMTP Server Settings:** (For the purpose of the lab, all configurations will be set to basic settings, which can later be modified and advanced as needed.)
Local host name should be exact same as your computer/server's name. Define SMTP Server Ports: Standard ports are 25 (unencrypted), 587 (encrypted/TLS), and 465 (encrypted/SSL).

- **Authentication** (our Lab environment is secure; we can bypass the SMTP authentication)

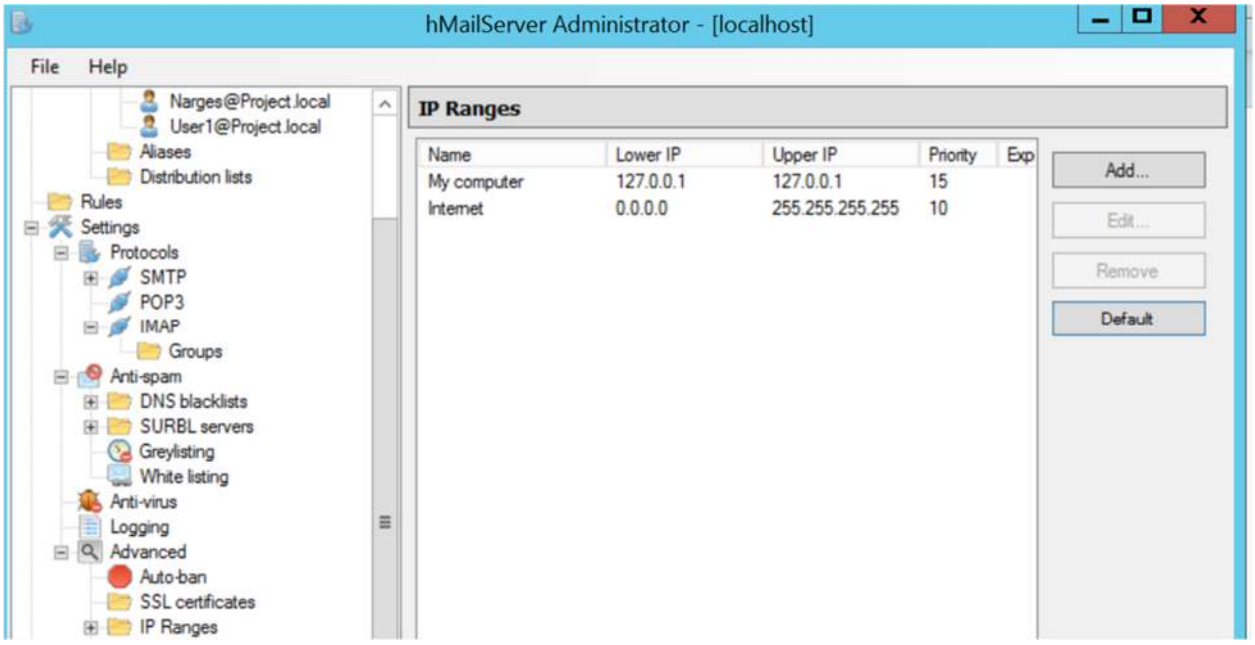


For this lab we will uncheck the SMTP authentication, no need.

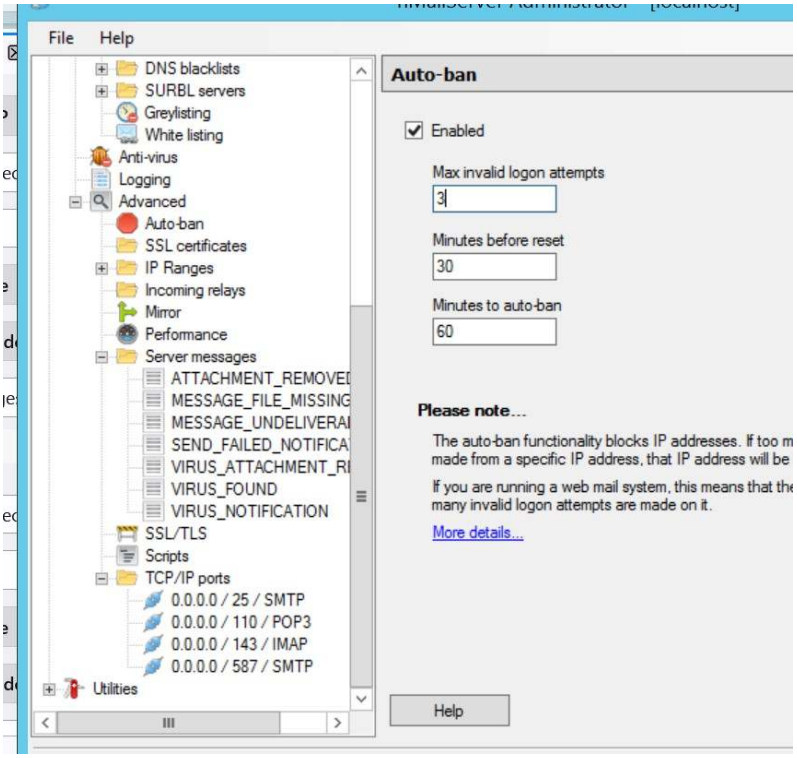



**Review some additional features and configs:**

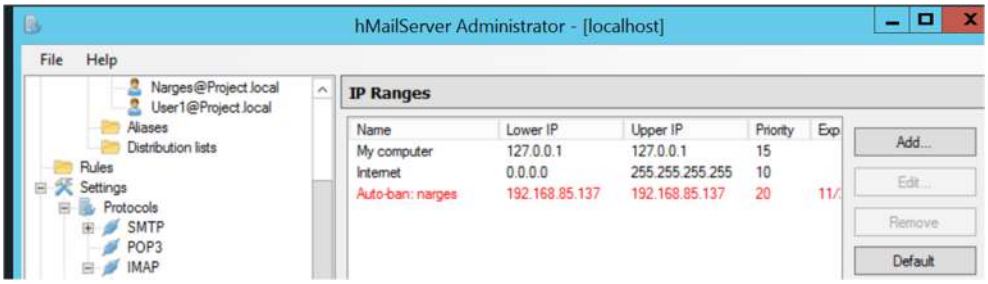
hMailServer is giving us the ability to limit the IP address:



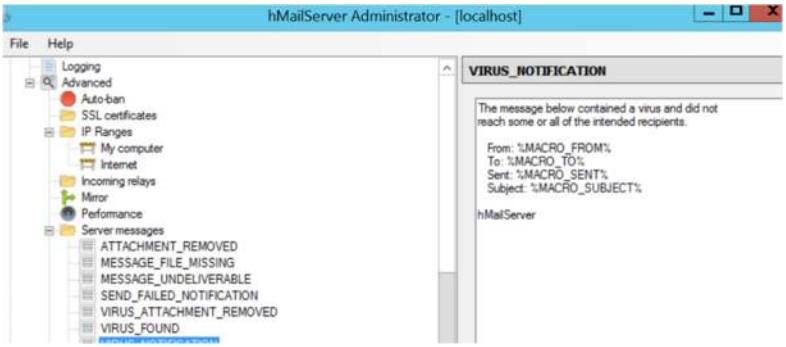

- One if the useful security features is Auto-ban feature, it will ban the IP Address of a system which have failed-attempt.



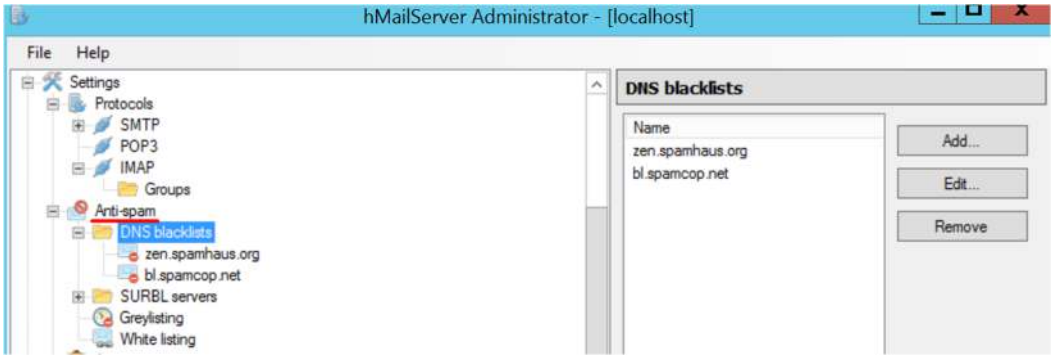

And if an IP get banned you can view, ban or un-ban it from here:



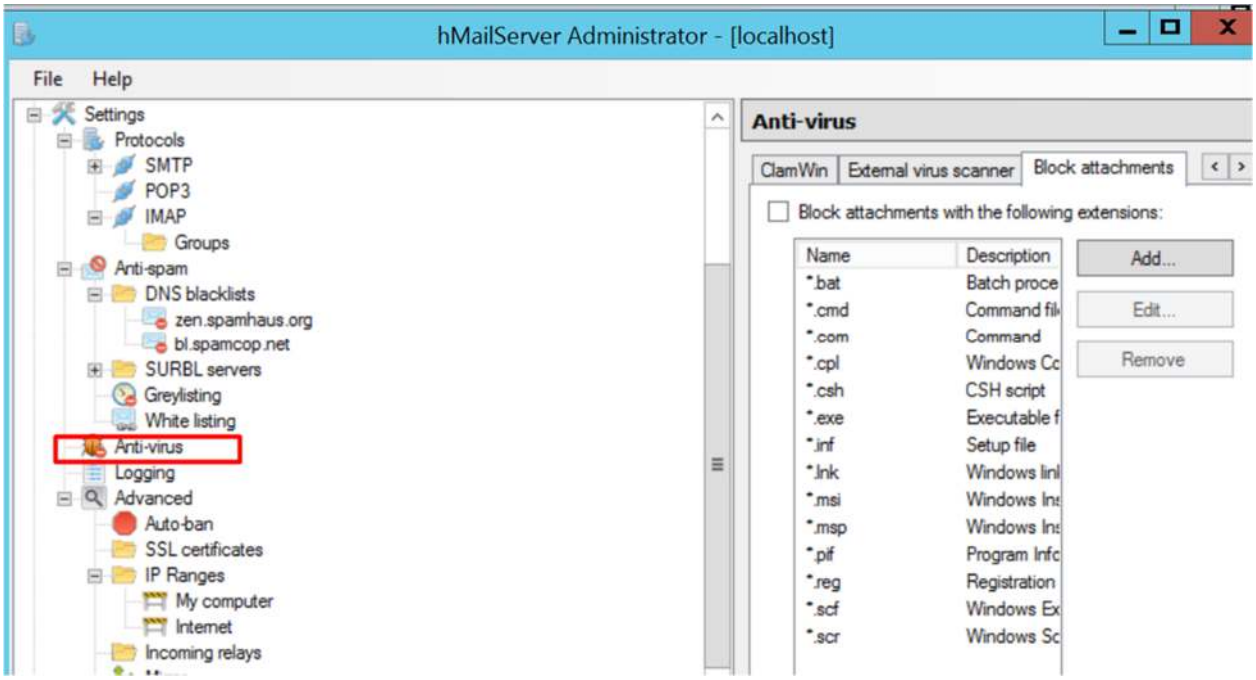

Setting up server messages in case on Virus detection, Missing files…



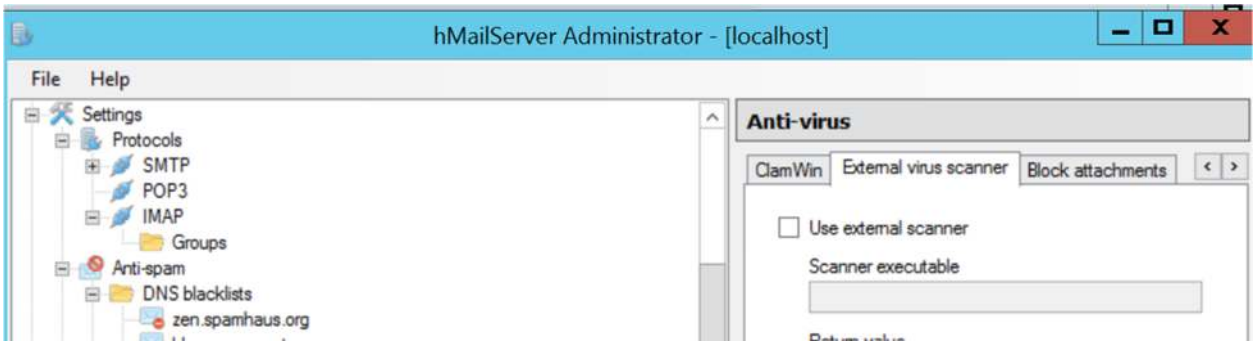
Ability to set up Spam list, Whitelisting a domain.



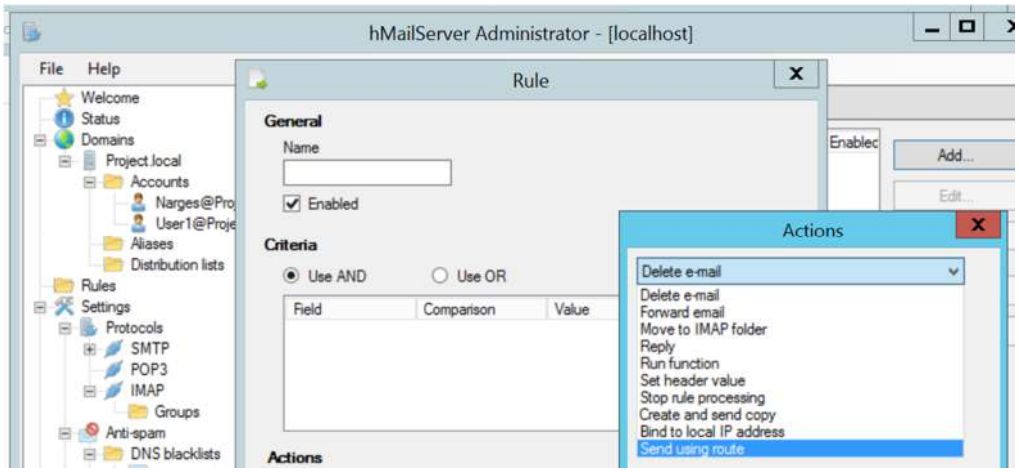

Setting up and defile the file type Anti-Virus should check.



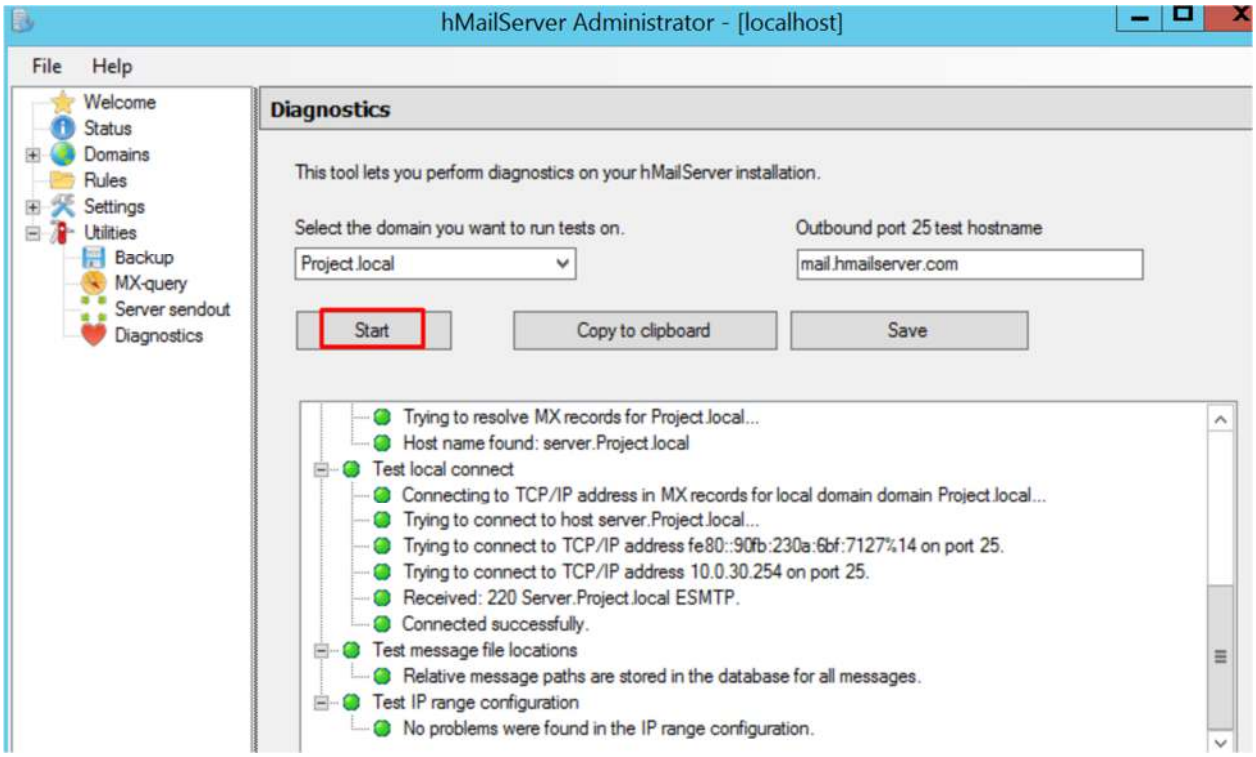

Or add any External Anti-Virus.



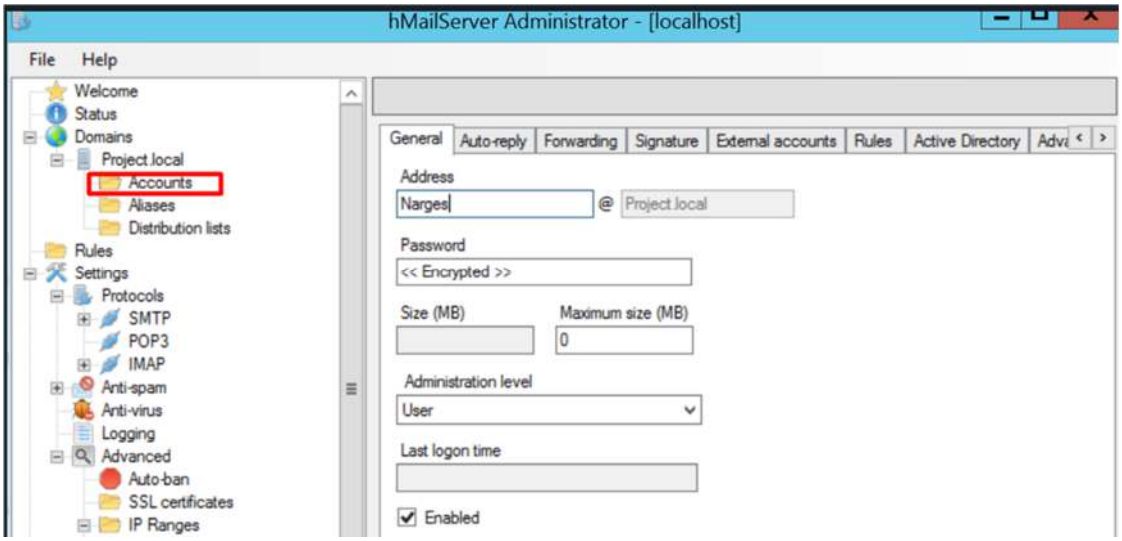
Setting up all type of Email Rules:

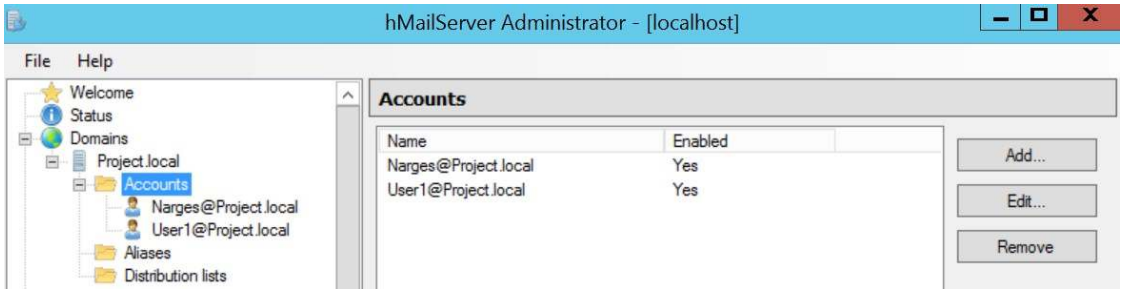



**Running the Diagnostics tool to make sure our server has configured properly.**



Server is ready and we'll start adding our Email accounts and save it.

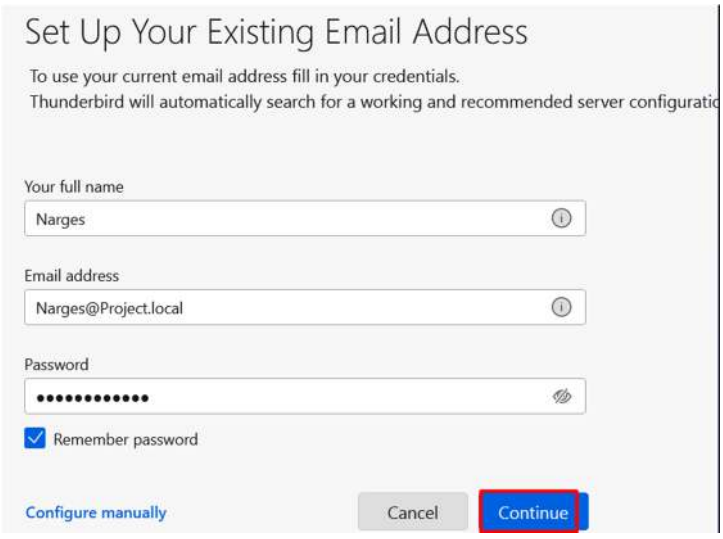


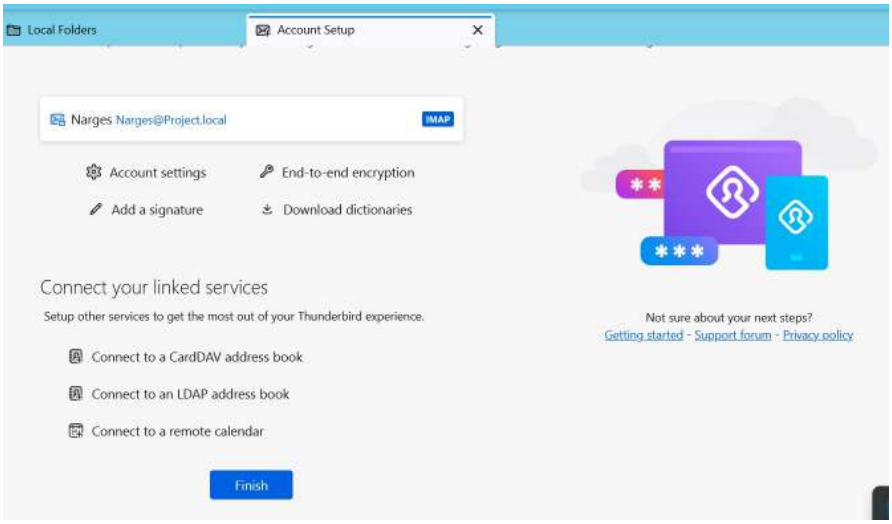

**Install/Configuration of Mail Client:**

For this project I'll use Thunderbird Mail clients which serve as software applications designed to access and manage email accounts. You can use other Mail clients such as Gmail or Outlook.

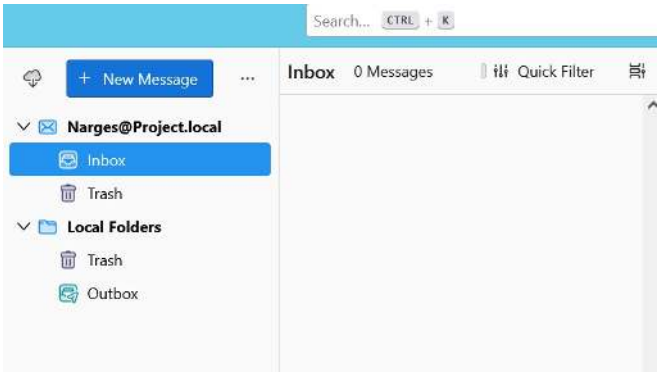
After installing the Thunderbird, you can lunch the application and start adding your Email account.



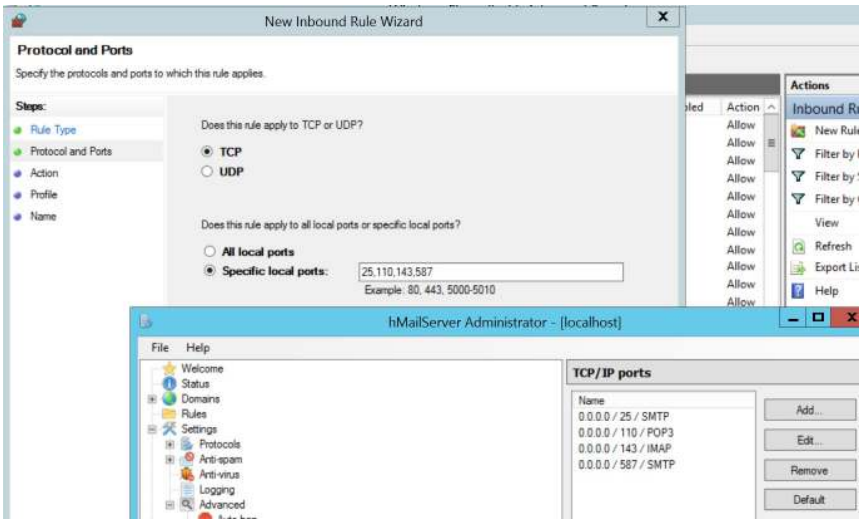
Continue and the Mail Client will be able to automatically find the Mail Server.




Email account is added and ready to receive the Emails.



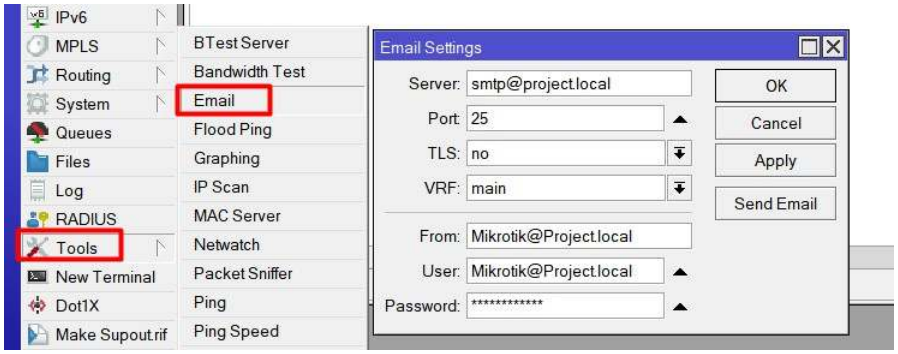

In case your Mail client is on another system, you need to make sure all required ports for incoming and outgoing traffic has been opened on your Server and Client host.



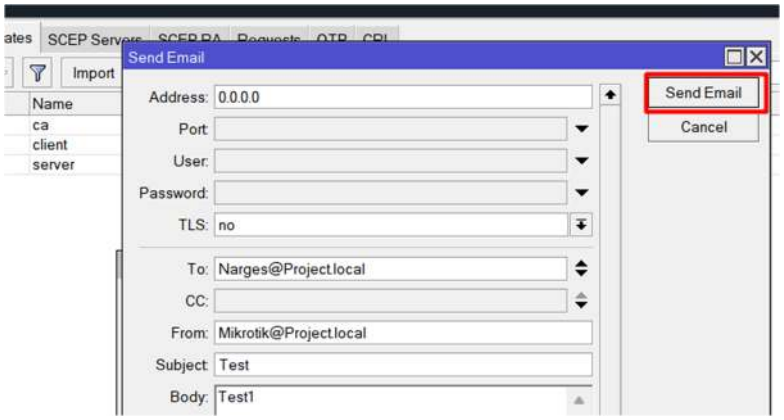
We've successfully installed our email server, and now we can leverage it in our topology by configuring email alerts on our router/firewall.

**Email Alert:**

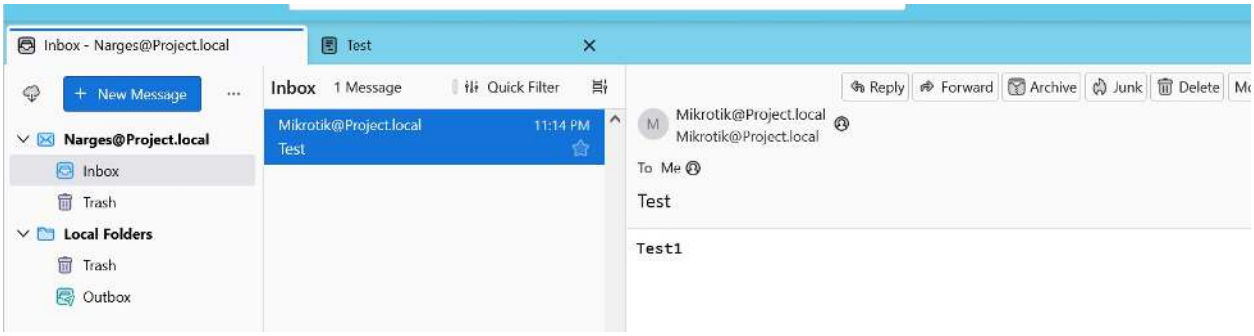
We have already added another account in our Mail server for Mikrotik router. ( Mikrotik@Project.local). We will configure the Email Address : Tools > Email > Outgoing server address …




Click on Send Email for testing the outgoing email.

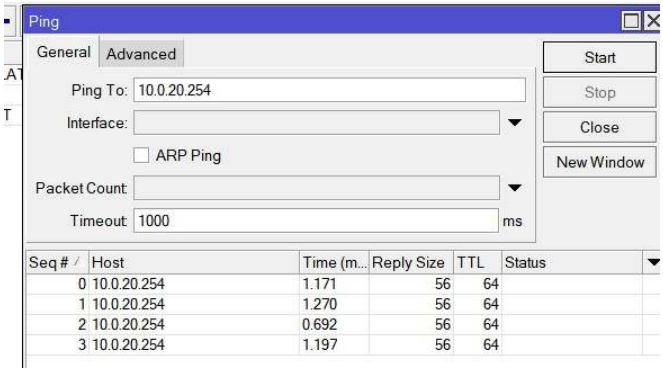



We can verify we have successfully received the Email on Narges@Project.local

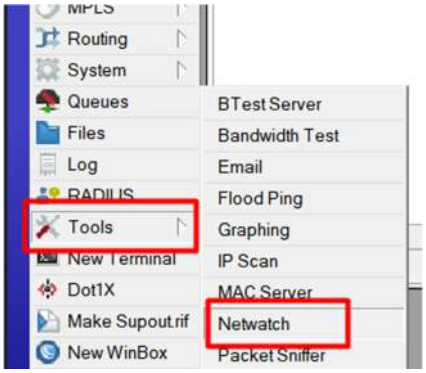


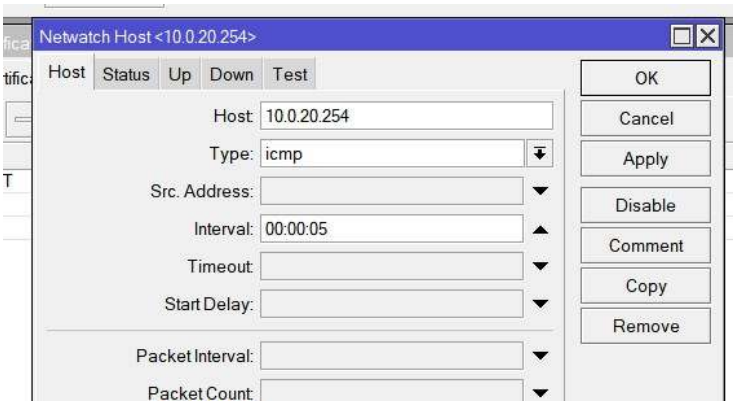
**Network Monitoring/Netwatch**: is a tool available on MikroTik routers that allows you to monitor the reachability of a host (usually an IP address) and take specific actions based on the results, for example can be used for failover in the Network. Netwatch continuously pings the specified host and performs actions when the ping status changes. Here's how it can works:

For testing purpose, I have chosen a host in VLAN 20: First need to make sure we can ping the host.



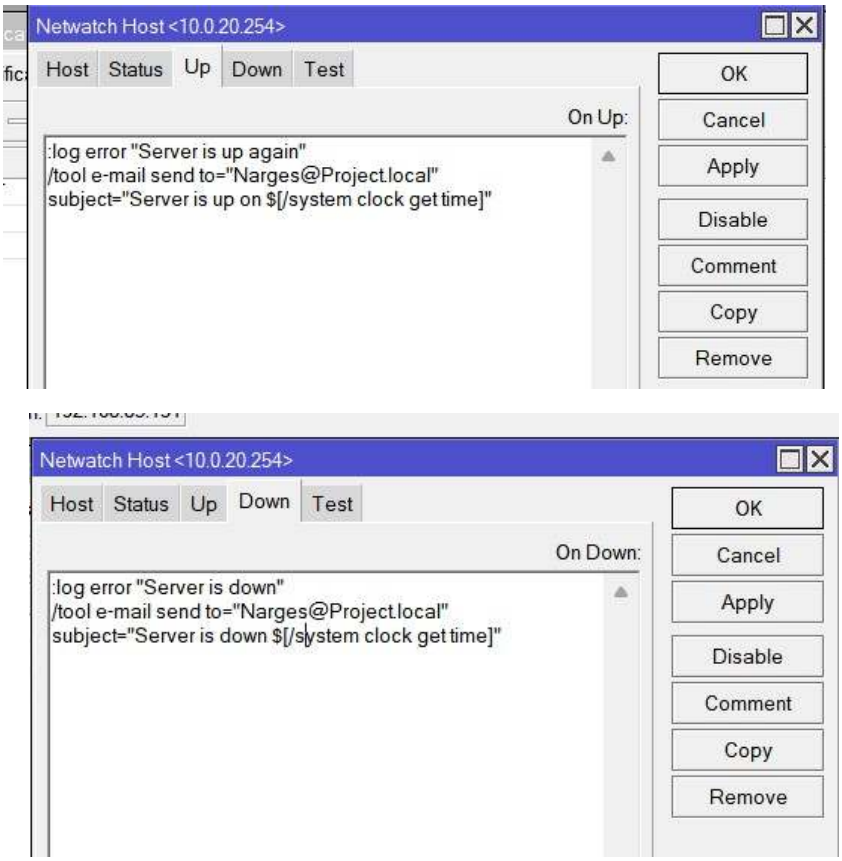

Set it up a new Netwatch host:



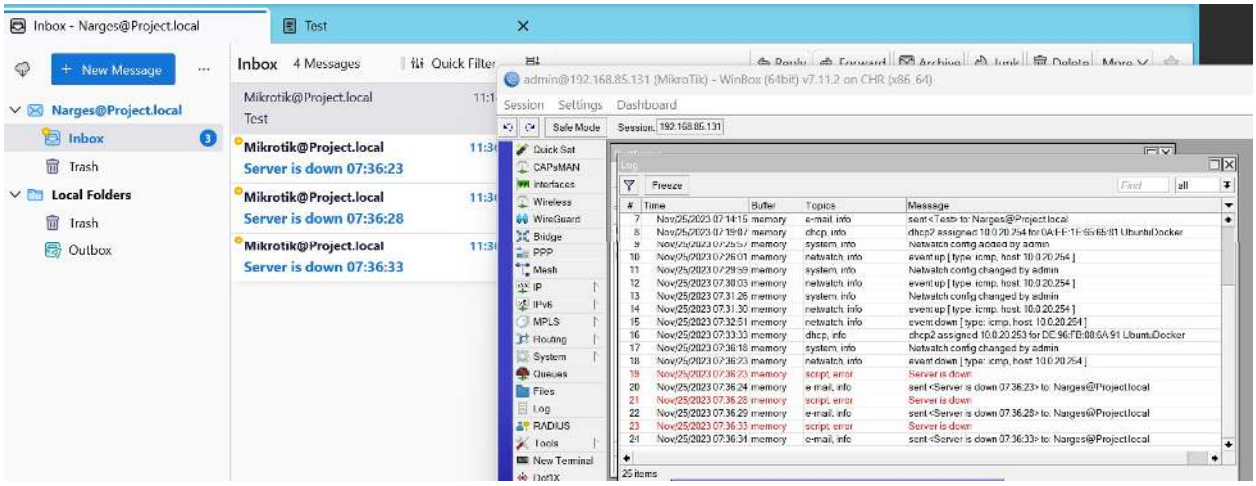

We need to write rule for the Email Alerts:

- :log error "**Server is down**" /tool e-mail send to="YourEmailAddress@gmail.com" subject="Server is down $[/system clock get time]"
- :log error "**Server is up again**" /tool e-mail send to="YourEmailAddress@gmail.com" subject="Server is up on $[/system clock get time]"




Netwatch rule has been added:


For testing purposes, tried to turn off/on the target host and successfully received the Email Alert on its set up interval.



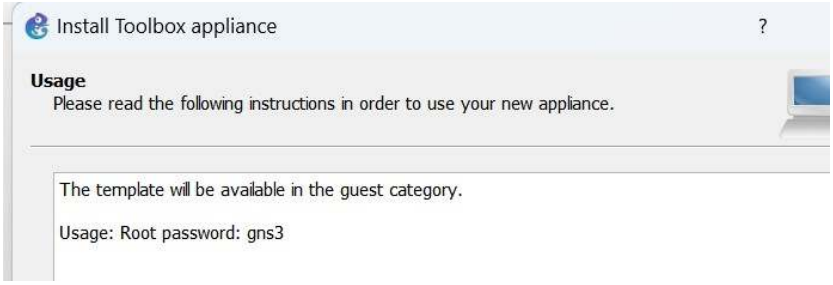
**FTP / TFTP Server/ Web Server /Syslog Server/ SNMP Trap receiver**

These services have been installed on a Linux system and imported to the topology taking the advantage of Networkers toolkit.

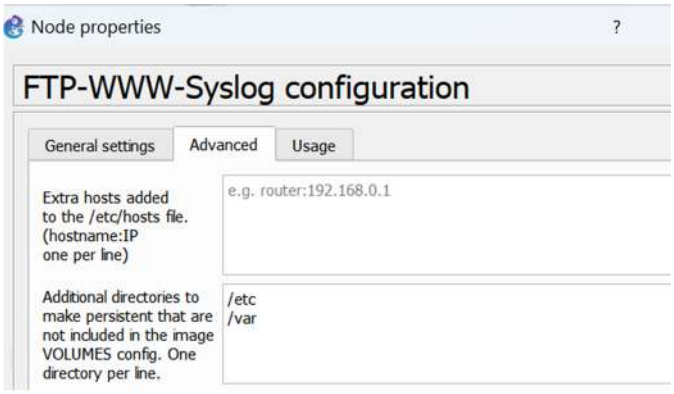
Here is how to import Networkers Tools appliance:

Download the toolbox from this link: [https://gns3.com/marketplace/appliances/networkers-toolkit](https://gns3.com/marketplace/appliances/networkers-toolkit)

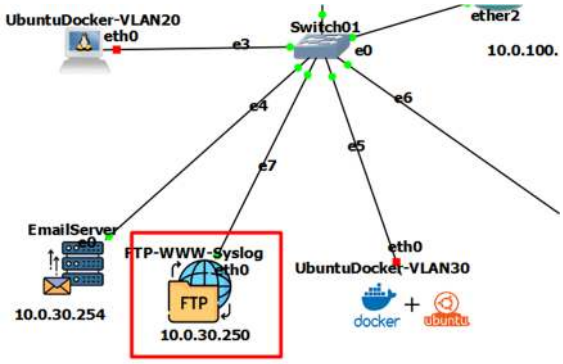
Import the appliance and install it on GNS3 VM, and will be available under guest devices.



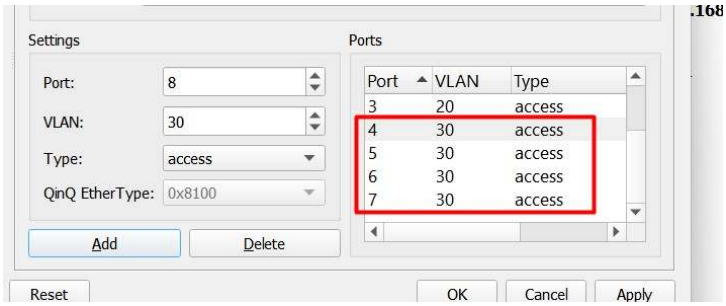

Once added to your topology same as other end devices, make the /etc /var directory persistent.



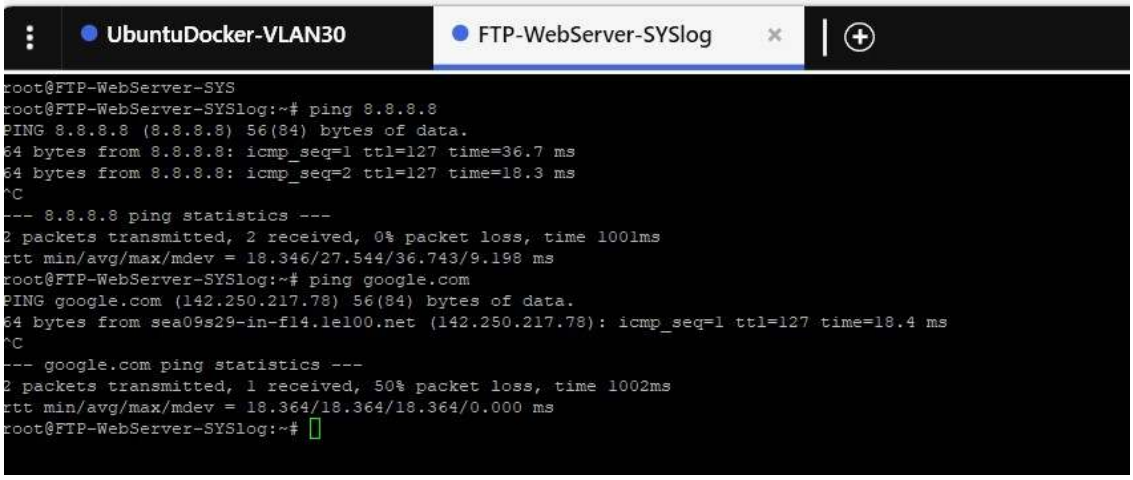

Recommended to assign static IP as we need a fix IP address to connect to our FTP Server/Web Server…



Double check the Switch ports to make sure devices/servers are in the right VLAN.



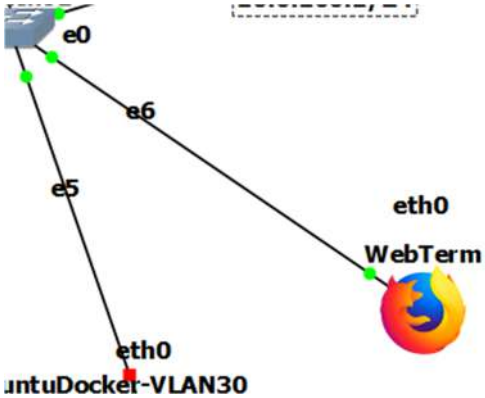

Verify the internet connectivity:



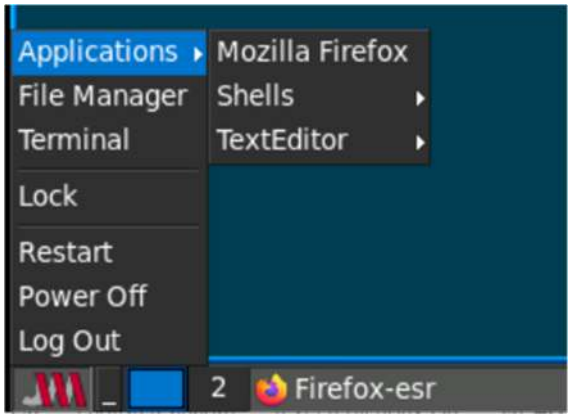

Web Server Files are configured under /var/www/html Directory.

To verify connectivity to the Web Server, I have added **WebTerm appliance** to the topology.

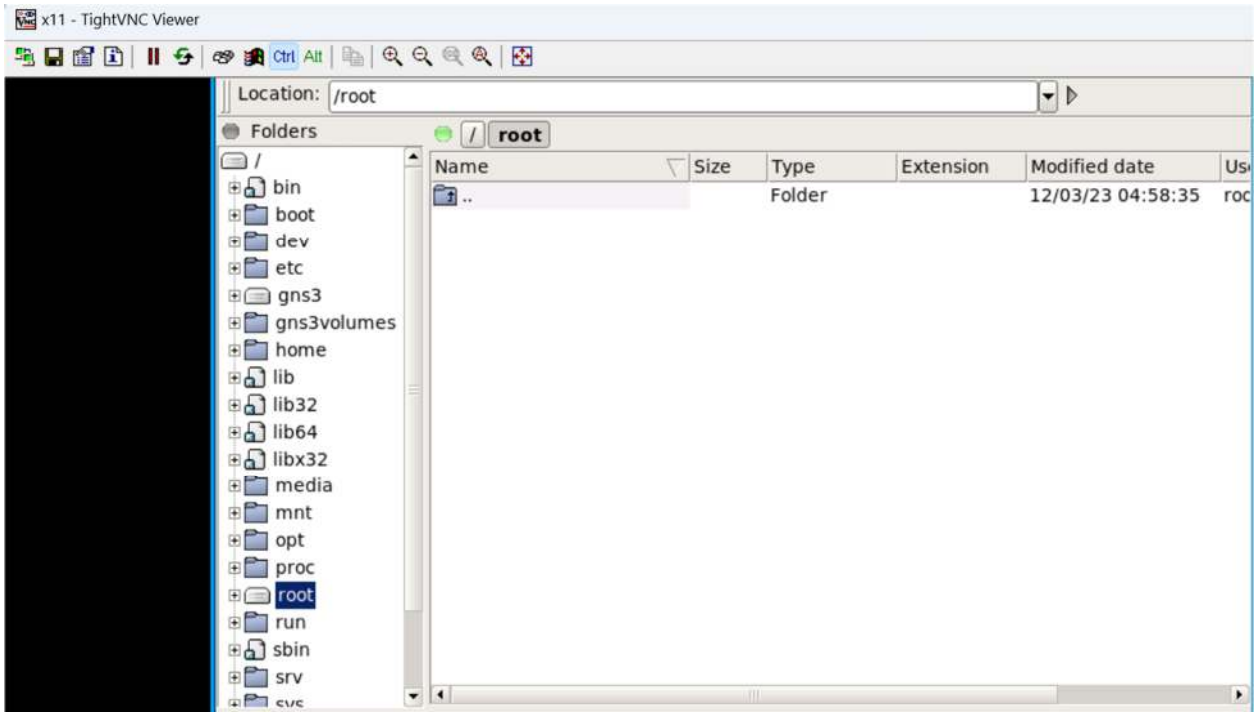
**Webterm appliance:** the WebTerm appliance is a virtual appliance that provides a web-based terminal interface for device management. his appliance is designed to facilitate command-line access to network devices using a web browser. Users can interact with the virtual devices in GNS3 through this web-based terminal.



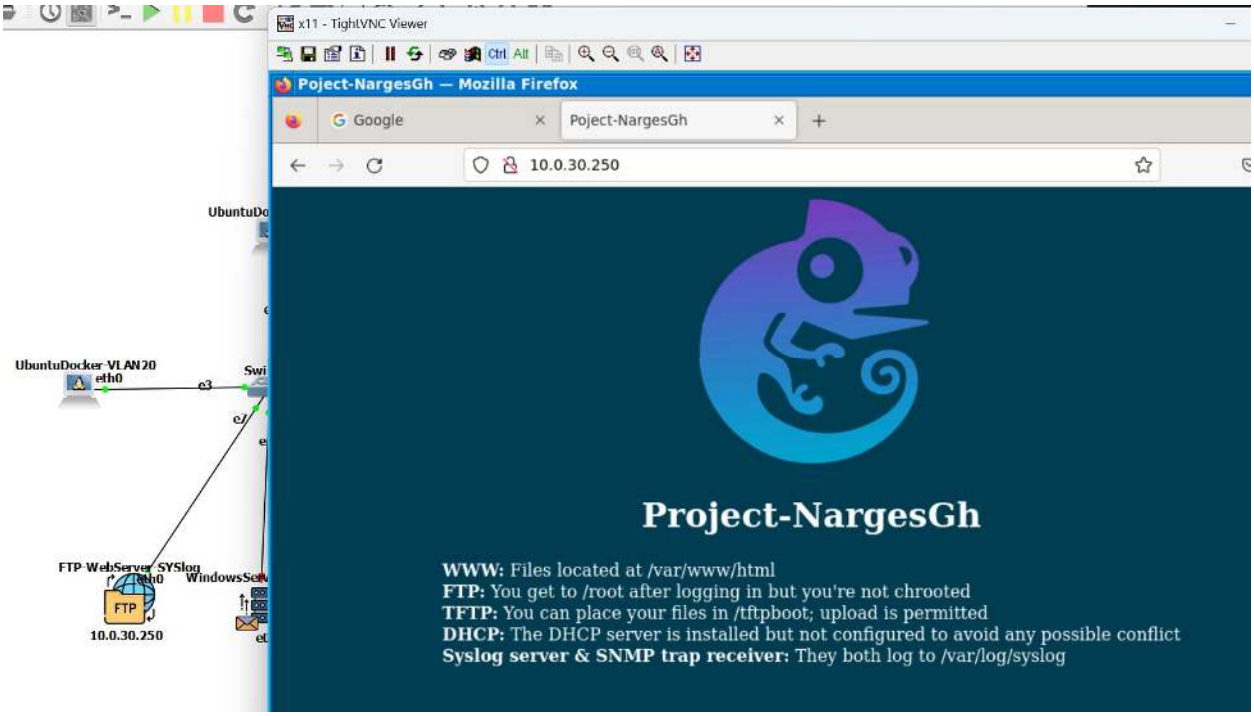
Right click on the WebTerm, Start > Console > you will connected to the WebTerm Linux box using TightVNC. WebTerm will provide you a Firefox browser, Xfe File manager , Terminal




**Xfe File Manager:** a lightweight and fast file manager for Unix-like systems. It is designed to provide a graphical user interface (GUI) for navigating and managing files and directories on a computer. Xfe stands for X File Explorer.




Now we will open the Firefox browser on WebTerm and will browse the IP address of the Networker Toolkit device ( Host of our WebServer), and we can verify that the WebServer is functional.



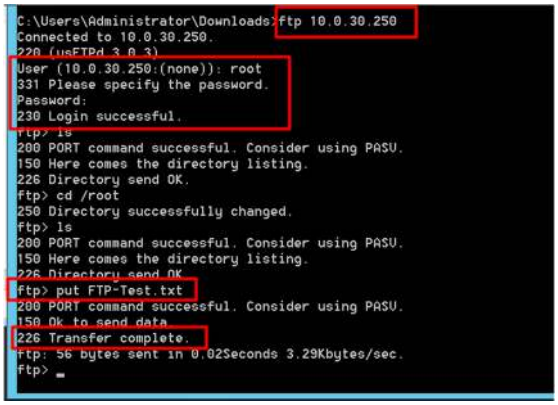

**FTP Connection/Upload file:**

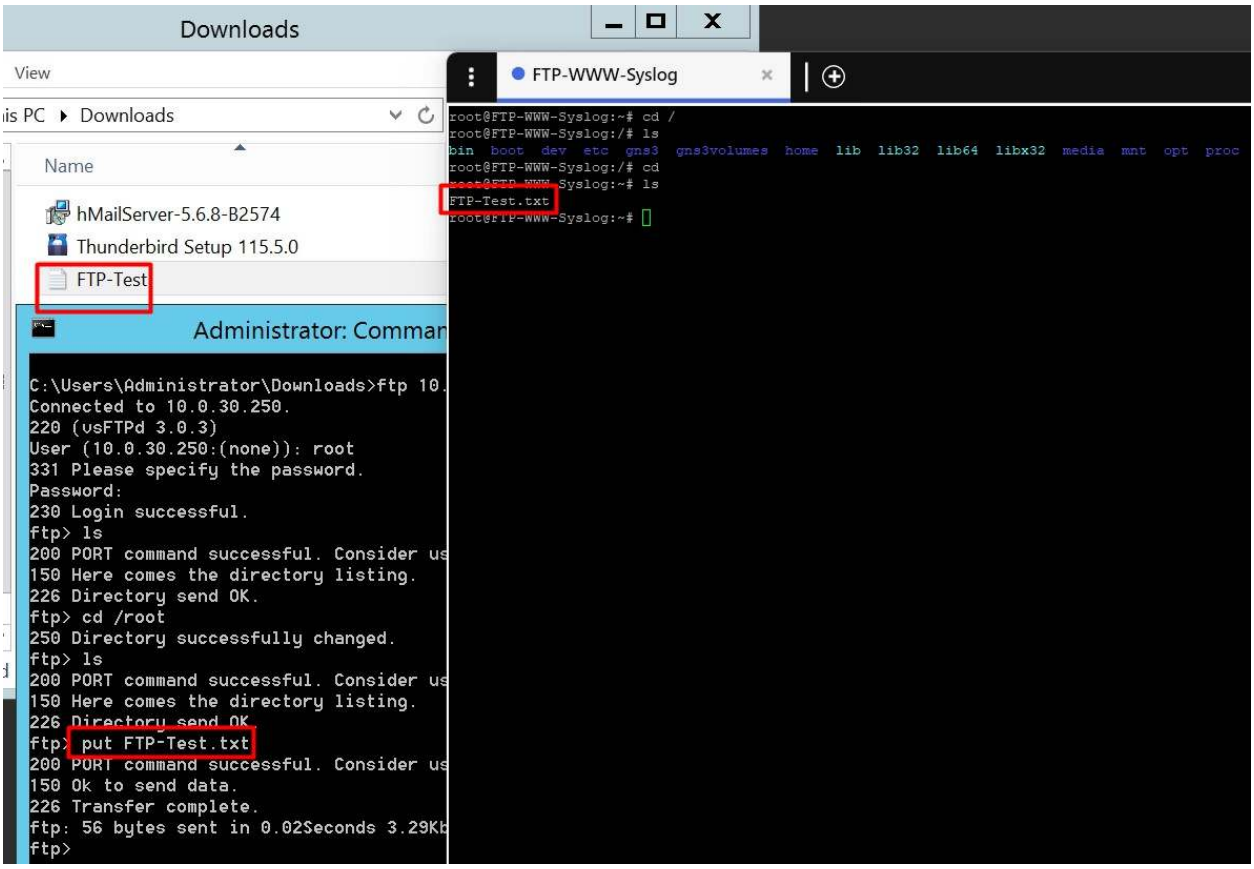
Right click on the FTP Server (Networker toolkit) > Console >


I used windows server as FTP Client > cmd > run FTP command and connect to the FTP server : 10.0.30.250.

User: root Password: gns3

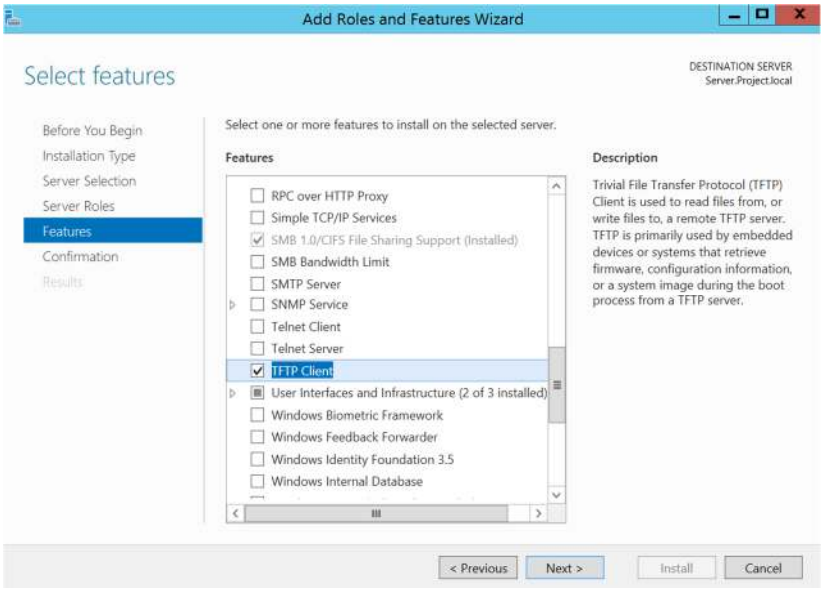
Upload a sample file and verify if it is under /root directory. Please note you do need to be in the directory of the file which need to be transferred to the FTP server.

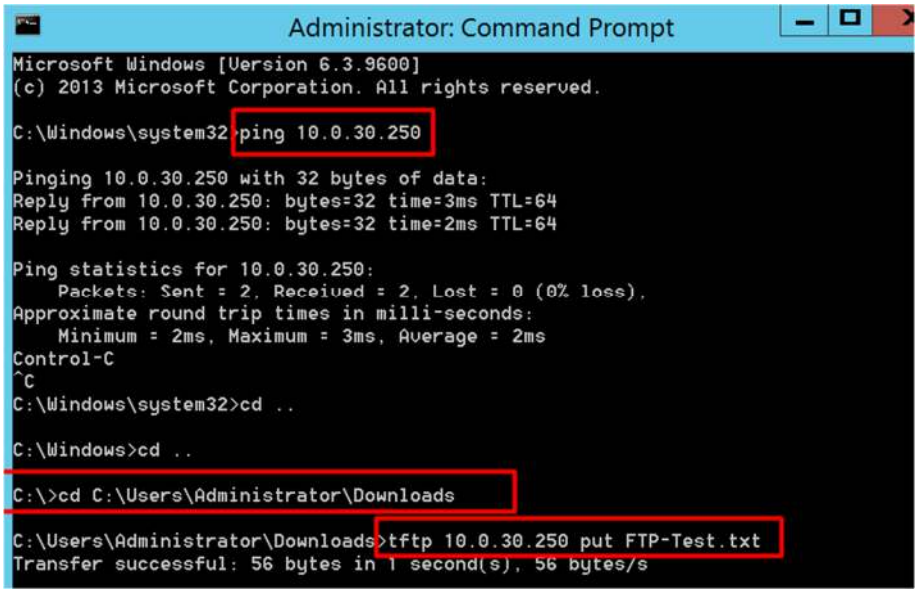




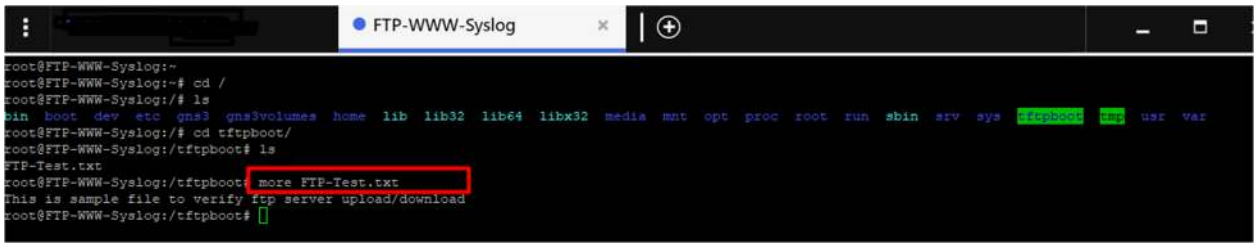

**TFTP Sever/Client:**

For TFTP client I have installed TFTP rule in Windows Server:






We observe the File has been transferred to tftpboot directory. And with more command we can read the content of the file.

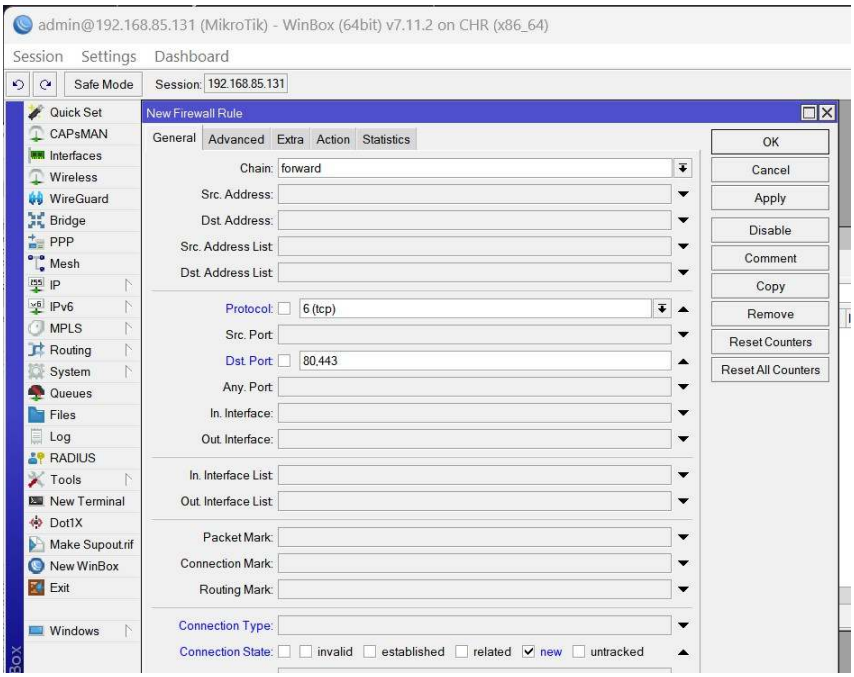


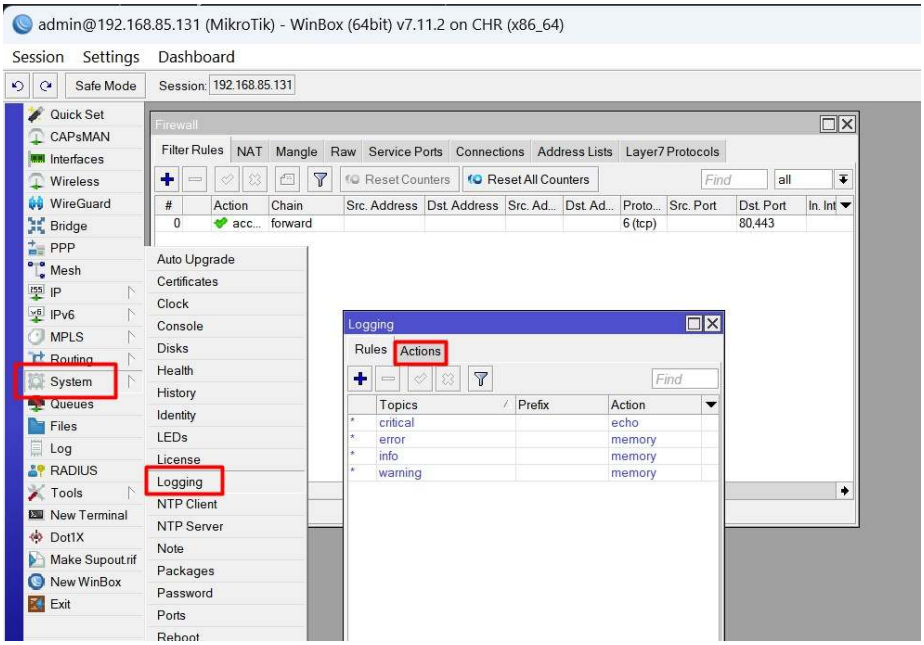

**Syslog Server:**

Syslog is a standard protocol used for the forwarding of log messages in an Internet Protocol (IP) network.A remote syslog server, often referred to simply as a syslog server on another server, is a centralized logging server that collects and stores log messages from various devices and applications within a network.

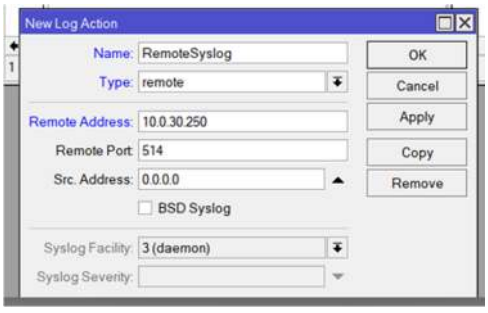
**Mikrotik Router configuration to log messages/events on our Syslog Server:**

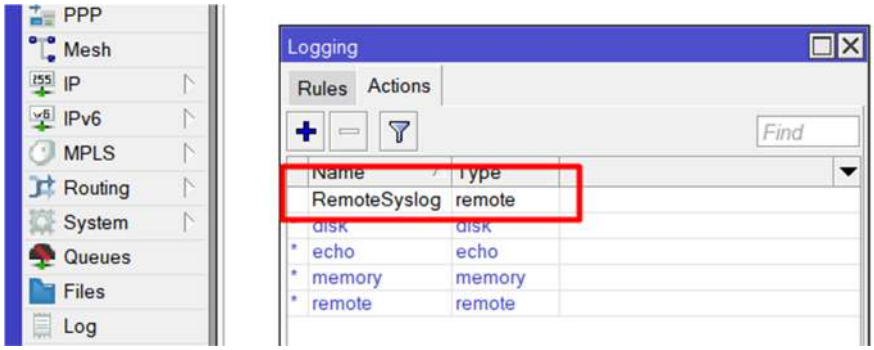
- Adding firewall rule
- Setting up logging action/rules



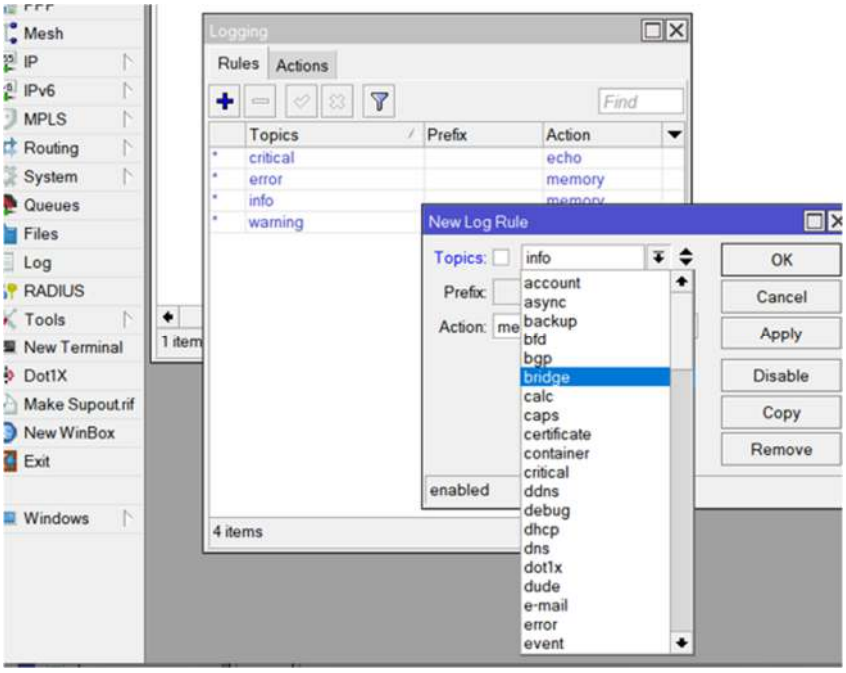



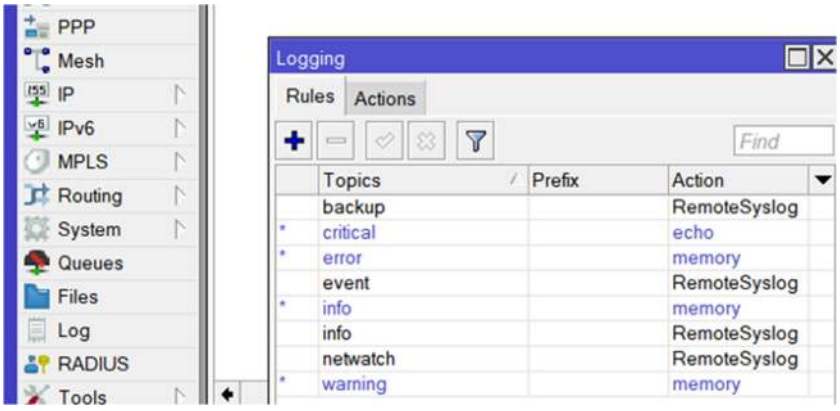

- **+** New log action**,** Remote address = Syslog server IP , Port = Syslog port



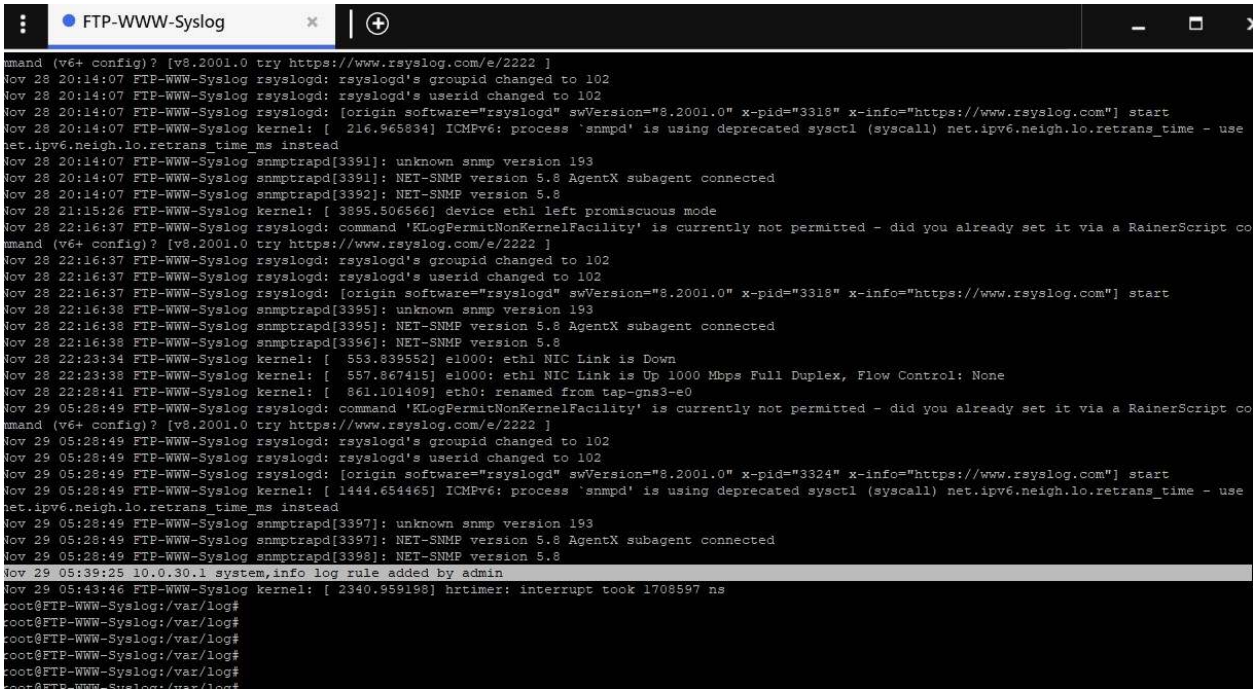



Next we will add own rule, to define what needs to be logged on remote syslog server.

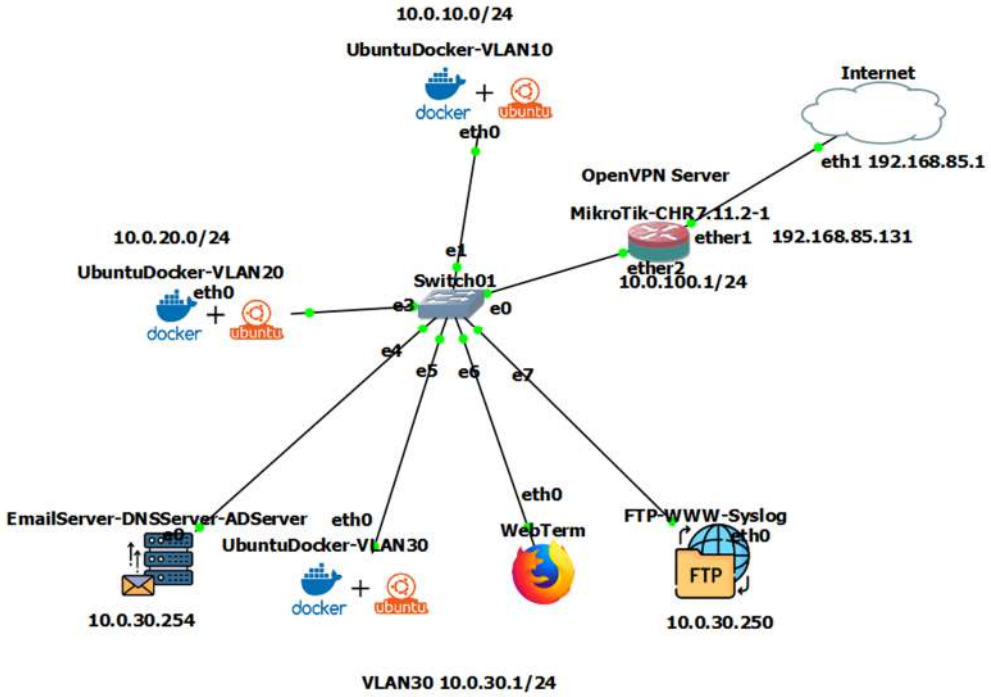


Now we will add/remove a rule to see has been logged on remote syslog server **under /var/log directory.**




**Topology Diagram:**



**Conclusion**

In conclusion, this report outlines a detailed walkthrough of a cost-free building and configuring a robust network environment using various tools and technologies. Starting with the foundational elements of virtualization, this document delved into the installation and integration of critical components such as the Cloud Hosted Router (CHR), OpenVPN, Email Server, and Networker Toolkits. Each step, from choosing the virtualization platform to configuring specific services like DHCP, DNS, and firewalls, has been meticulously covered.

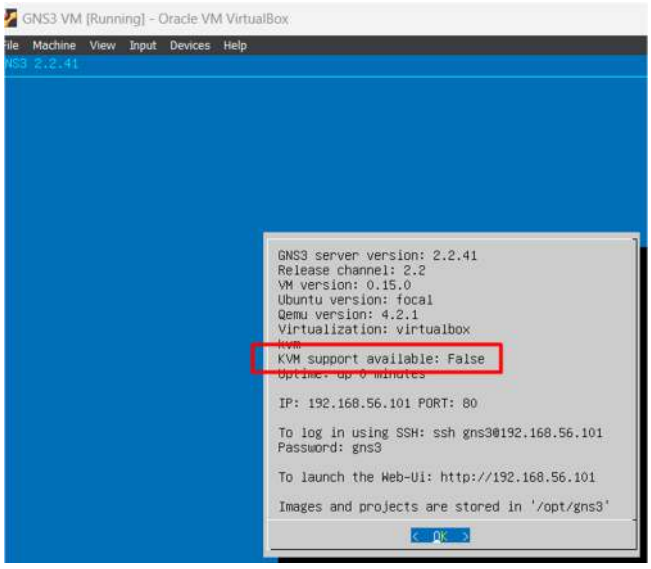
**References**


1. Getting started with GNS3. GNS3 Documentation. (n.d.). https://docs.gns3.com/docs/
2. Cloud hosted router, CHR - RouterOS - MikroTik documentation. (n.d.). https: https://help.mikrotik.com/docs/
3. Overview of the get started guide." (2023, August 23). Docker Documentation. https://docs.docker.com/get-started/
4. Bonaventure. (2015). Computer Networking: Principles, Protocols, and Practice. 1st ed. CreateSpace Independent
Publishing Platform. ISBN: 9781329342697.

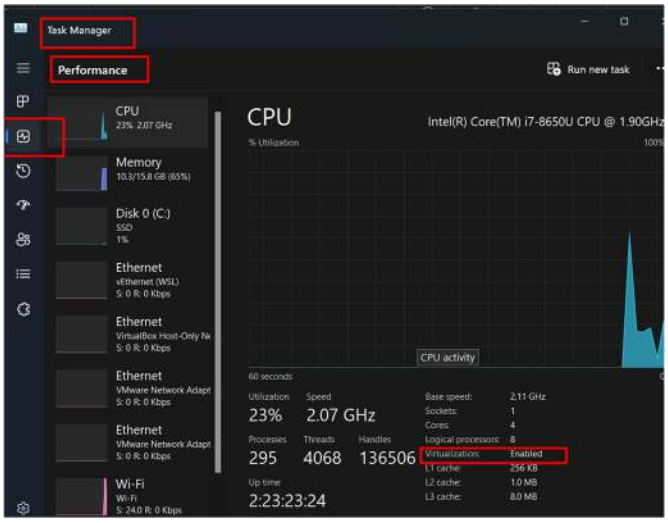

**Appendix**

The appendix contains troubleshooting information related to virtualization issues, ensuring a guide for users facing challenges during implementation.

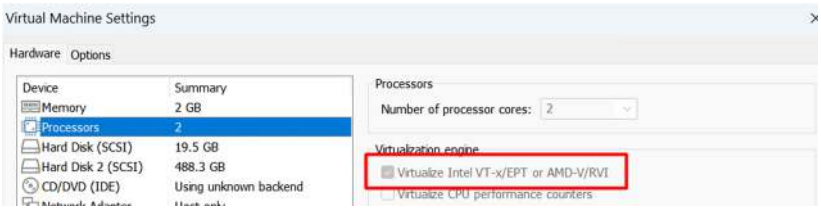
In case you encounter an error and find that "**KVM Support Available" is marked as False**, please follow the steps in the Appendix to resolve the issue.




Things to check include ensuring that virtualization is enabled in your system's BIOS settings.

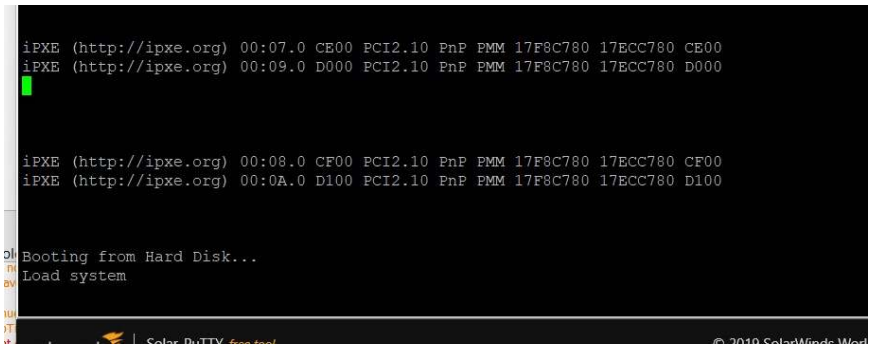



Additionally, make sure that in your VM processor settings, the VT-X or V/RVI feature is enabled.

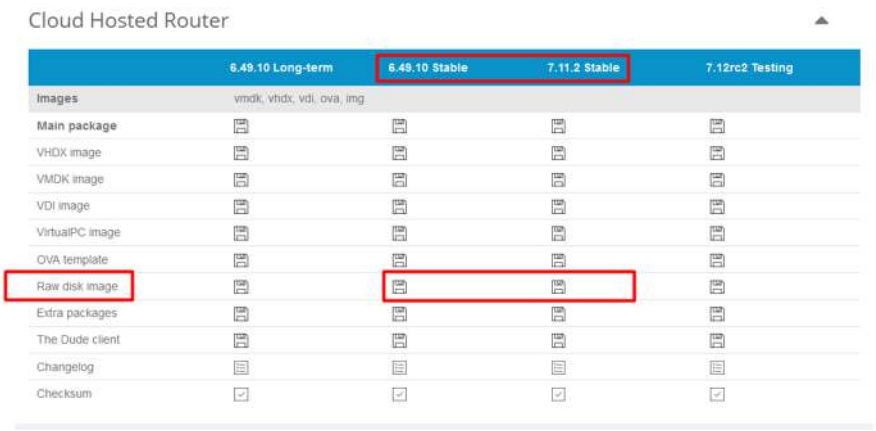



**Error:** CHR on startup would install all the software If you faced a loop while booting make sure you have chosen a stable version.

**Loop issue >**




https://mikrotik.com/download




- If you constantly got error the Email server not found, check the Baned IPs under, and remove the IP.