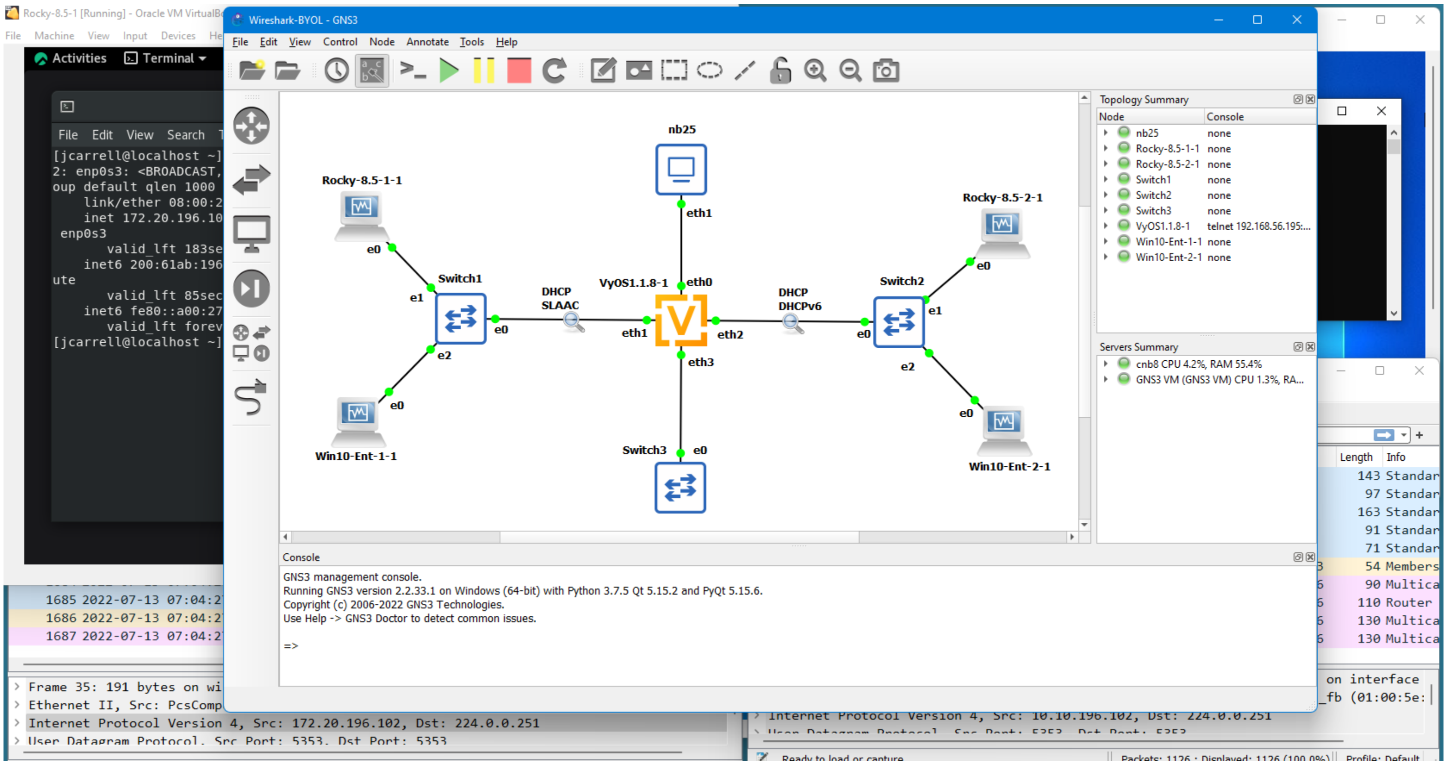
Welcome to the Build Your Own Wireshark Learning Lab for Free - Workshop



```
[jcarrell@localhost ~]
2: enp0s3: <BROADCAST,
oup default qlen 1000
    link/ether 08:00:2
    inet 172.20.196.10
 enp0s3
       valid_lft 183se
    inet6 200:61ab:196
ute
       valid_lft 85sec
    inet6 fe80::a00:27
       valid_lft forev
[jcarrell@localhost ~]
```

Node	Console
nb25	none
Rocky-8.5-1-1	none
Rocky-8.5-2-1	none
Switch1	none
Switch2	none
Switch3	none
VyOS1.1.8-1	telnet 192.168.56.195:...
Win10-Ent-1-1	none
Win10-Ent-2-1	none

```
cnb8 CPU 4.2%, RAM 55.4%
GNS3 VM (GNS3 VM) CPU 1.3%, RA...
```

```
GNS3 management console.
Running GNS3 version 2.2.33.1 on Windows (64-bit) with Python 3.7.5 Qt 5.15.2 and PyQt 5.15.6.
Copyright (c) 2006-2022 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=>
```

```
1685 2022-07-13 07:04:2
1686 2022-07-13 07:04:2
1687 2022-07-13 07:04:2

> Frame 35: 191 bytes on wi
> Ethernet II, Src: PcsComp
> Internet Protocol Version 4, Src: 172.20.196.102, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
```

```
143 Standar
 97 Standar
163 Standar
 91 Standar
 71 Standar
 54 Members
 90 Multica
110 Router
130 Multica
130 Multica

on interface
_fb (01:00:5e:
> Internet Protocol Version 4, Src: 10.10.196.102, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Ready to load or capture    Packets: 1126 · Displayed: 1126 (100.0%)    Profile: Default
```

Overview of lab procedures

- Install and configure VirtualBox and Extensions
- Import and configure GNS3 VM
- Install and configure GNS3
- Create VyOS router VM
- Configure VyOS
- Create 2 or more clients

Wireshark Build Your Own Lab: Table of Contents

I. Lab IPv4 & IPv6 Address Schema

1. Host computer = 10.1.199.1 and 200:61ab:199:1011::1
2. GNS3 VM = 10.1.199.101 (bridged to host interface above)
3. VyOS eth0 = 10.1.199.201 and 200:61ab:199:1011::201
4. VyOS eth1 = 172.20.1.1 and 200:61ab:1:201::1
5. VyOS eth2 = 10.10.1.1 and 200:61ab:1:1010::1
6. VyOS eth3 = 192.168.1.1 and 200:61ab:1:cafe::1

II. Obtain software

- If not already done so, download the following:

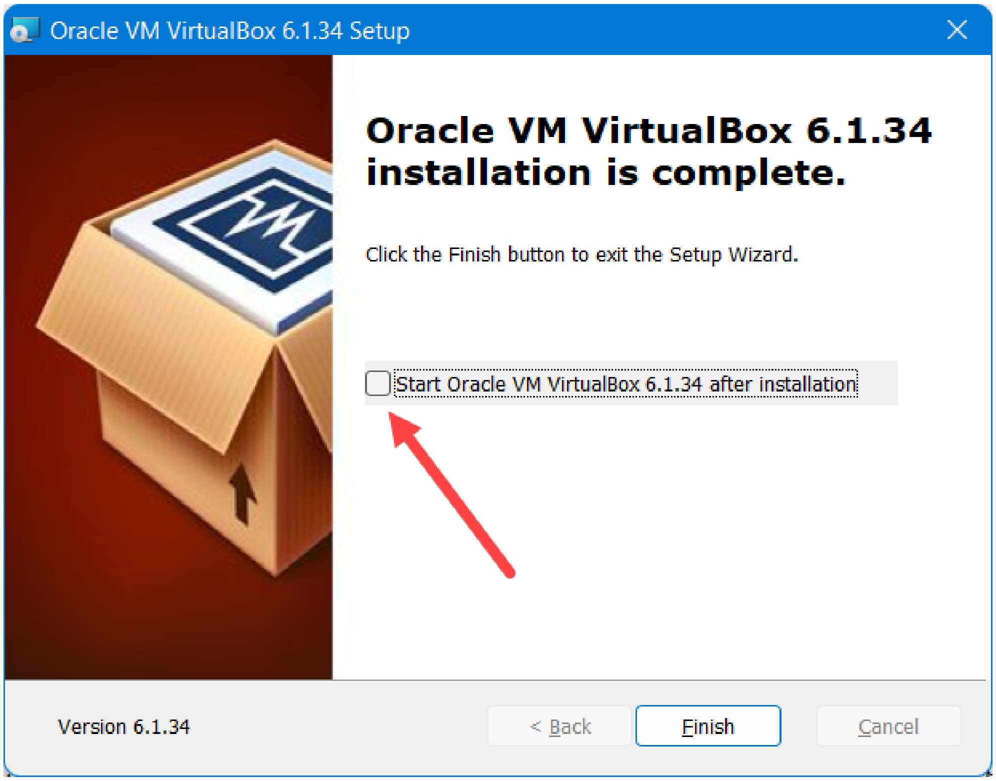
1. https://www.virtualbox.org/wiki/Downloads (select for your host OS)
2. https://download.virtualbox.org/virtualbox/6.1.34/Oracle_VM_VirtualBox_Extension_Pack-6.1.34.vbox-extpack
3. https://github.com/GNS3/gns3-gui/releases (select for your host OS)
4. https://github.com/GNS3/gns3-gui/releases/download/v2.2.33.1/GNS3.VM.VirtualBox.2.2.33.1.zip
5. https://s3.amazonaws.com/s3-us.vyos.io/vyos-1.1.8-amd64.iso
6. https://sourceforge.net/projects/gns-3/files/Empty%20Qemu%20disk/empty8G.qcow2/download
7. https://dl.rockylinux.org/vault/rocky/8.5/isos/x86_64/Rocky-8.5-x86_64-dvd1.iso
8. https://go.microsoft.com/fwlink/p/?LinkID=2195400&clcid=0x409&culture=en-us&country=US
9. http://old.kali.org/kali-images/kali-2021.1/kali-linux-2021.1-live-arm64.iso

III.Install VirtualBox

VirtualBox was chosen for the virtual machine platform as it is a free application, supports many different host OS's, but more importantly, it allows for having multiple network adapters and choosing different adapters for the various VM clients you may use

1. Navigate to directory where you copied the VirtualBox installer file and install VirtualBox (can accept the defaults options during install, or customize for your specific requirements)

   a) At the "Oracle VM VirtualBox installation is complete" untic the "Start Oracle VM VirtualBox 6.1.34 after installation" box (ie, do not start VB yet)



Oracle VM VirtualBox 6.1.34 Setup

Oracle VM VirtualBox 6.1.34 installation is complete.

Click the Finish button to exit the Setup Wizard.

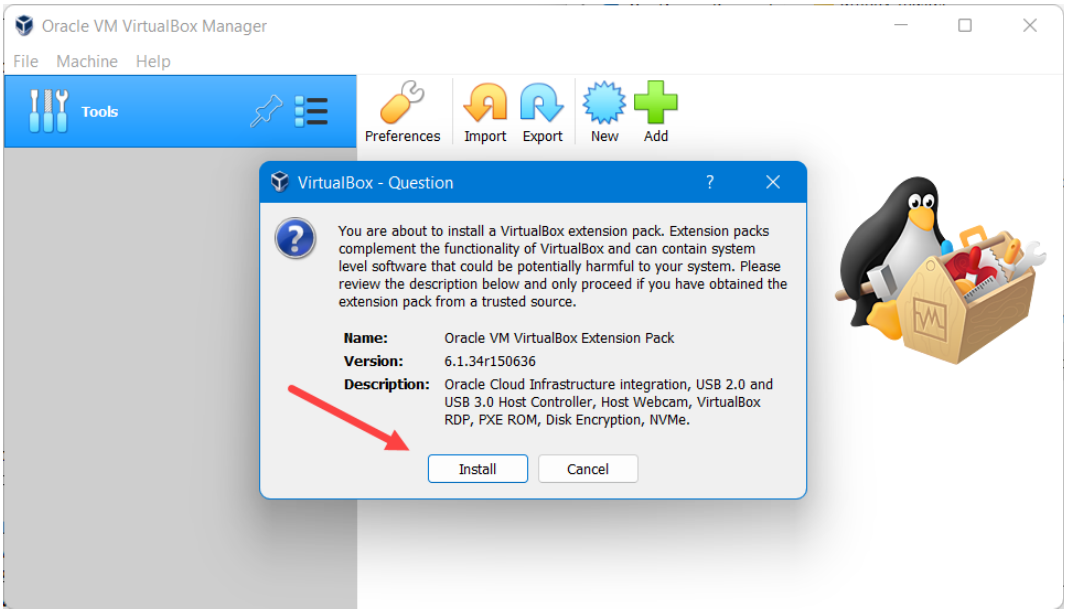
☐ Start Oracle VM VirtualBox 6.1.34 after installation

Version 6.1.34

2. Select finish

3. Install the VirtualBox Extension Pack

4. VirtualBox started and you are presented with a welcome screen

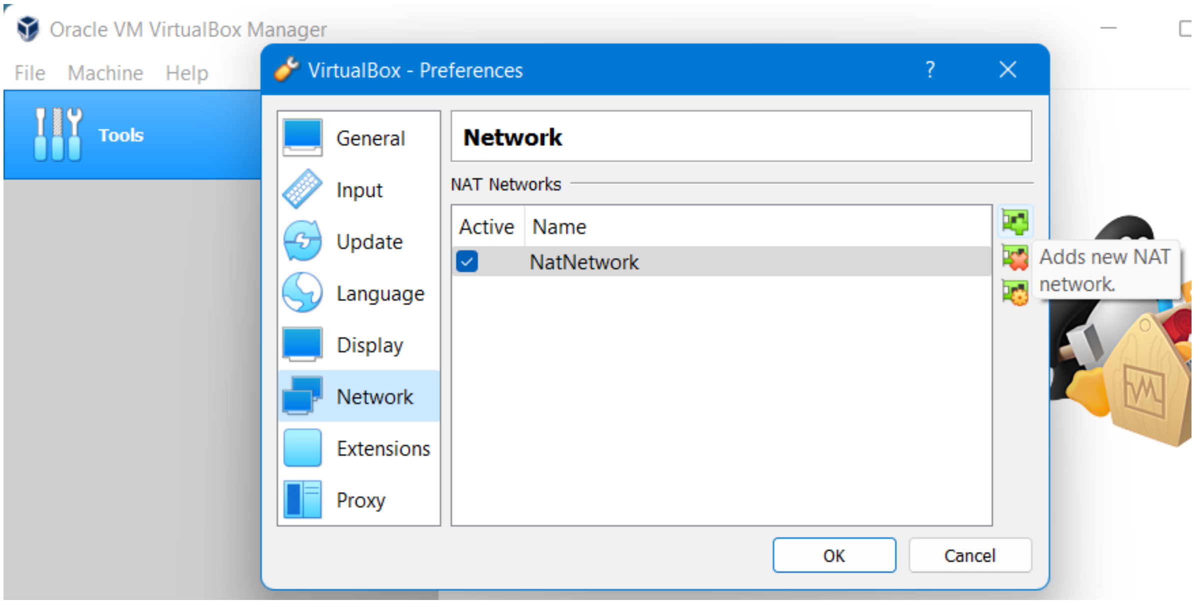


You are about to install a VirtualBox extension pack. Extension packs complement the functionality of VirtualBox and can contain system level software that could be potentially harmful to your system. Please review the description below and only proceed if you have obtained the extension pack from a trusted source.

Name: Oracle VM VirtualBox Extension Pack
Version: 6.1.34r150636
Description: Oracle Cloud Infrastructure integration, USB 2.0 and USB 3.0 Host Controller, Host Webcam, VirtualBox RDP, PXE ROM, Disk Encryption, NVMe.

5. Configure VirtualBox:

a) Add a NAT interface: >File >Preferences >Network >select the "+" symbol



Active	Name
☑	NatNetwork

b) Add a host-only network interface: >File >Host Network Interface >Create. After the interface has been created:

(1) select Properties and configure the IPv4 address to 192.168.56.1/24

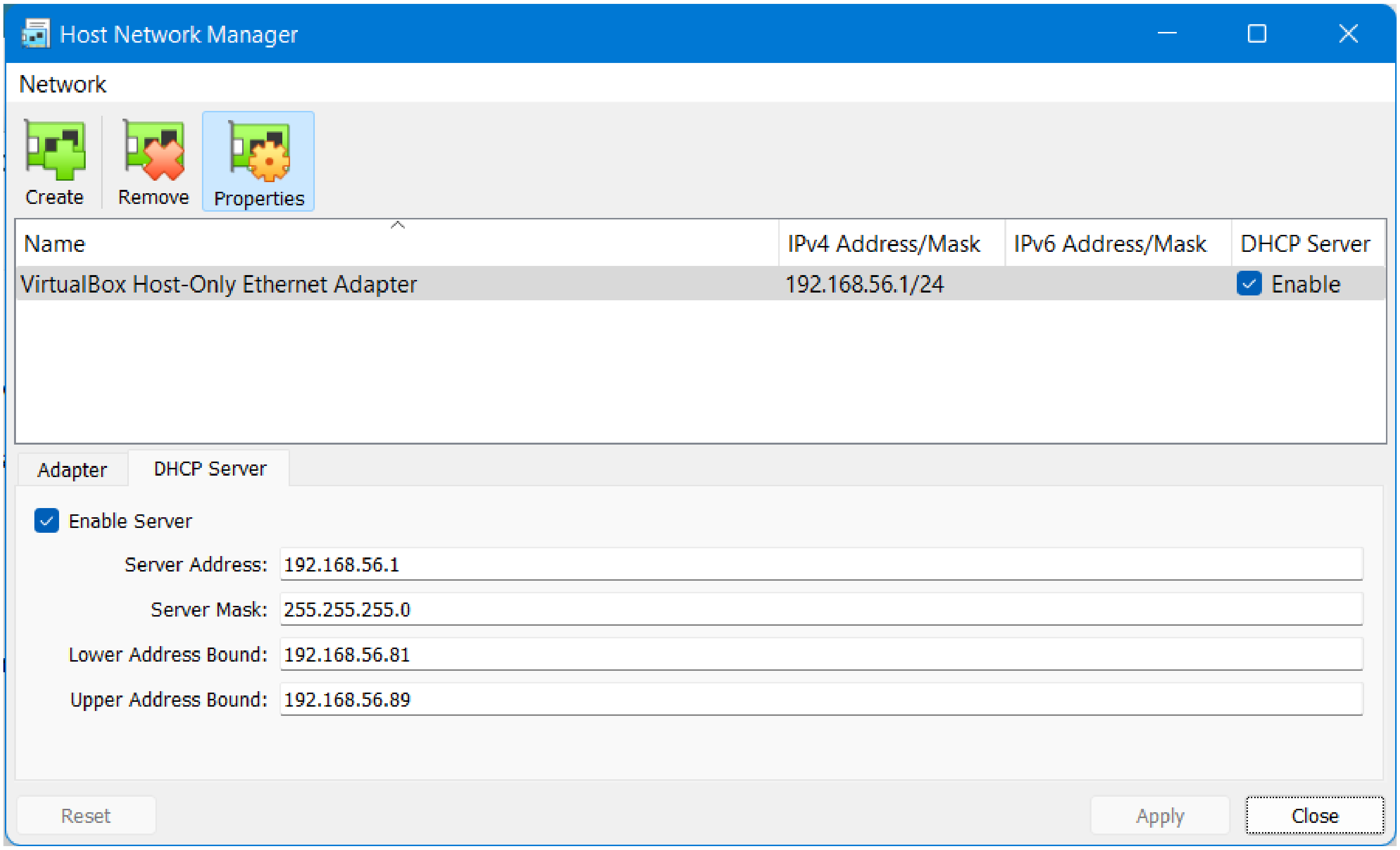
(2) select the DHCP Server tab, tic "Enable Server"

(3) Server Address = 192.168.56.1/24

(4) Lower Address Bound = 192.168.56.81

(5) Upper Address Bound = 192.168.56.89

(6) selecting "Apply" the screen will update to all the new settings



Name	IPv4 Address/Mask	IPv6 Address/Mask	DHCP Server
VirtualBox Host-Only Ethernet Adapter	192.168.56.1/24		☑ Enable

☑ Enable Server

Server Address: 192.168.56.1

Server Mask: 255.255.255.0

Lower Address Bound: 192.168.56.81

Upper Address Bound: 192.168.56.89

IV. Import and configure GNS3 VM

1. Import the GNS3 VirtualBox VM (note, the GNS3 VM must be the same version of GNS3 that will soon be installed)

   a) Extract the GNS3.ova from the GNS3.VM.VirtualBox zip file

   b) In VirtualBox, import the VM: >File >Import Appliance, navigate to select the GNS3.ova file

   c) Edit the Appliance settings:

      (1) RAM = 4G if host has 8G, or 8G if the host => 16G

      (2) CPU = 2

      (3) Both Network Adapters = "Intel PRO/1000 MT Desktop (82540EM)"

   d) Select Import (this may take up to ~ 5 minutes)

2. After the VM has been imported, select the Settings Icon

   a) >Network >Adapter 1 tab

      (1) Ensure the "Enable Network Adapter" box is tic'd

      (2) Ensure the "Attached to" is selected to "Host-only Adapter"

      (3) Select the "Advanced" dropdown

         (a) Promiscuous Mode = Allow All

   b) >Network >Adapter 2 tab

      (1) Ensure the "Enable Network Adapter" box is tic'd

      (2) Attached to = Bridged Adapter

      (3) Name = <the host system wired or wireless interface>

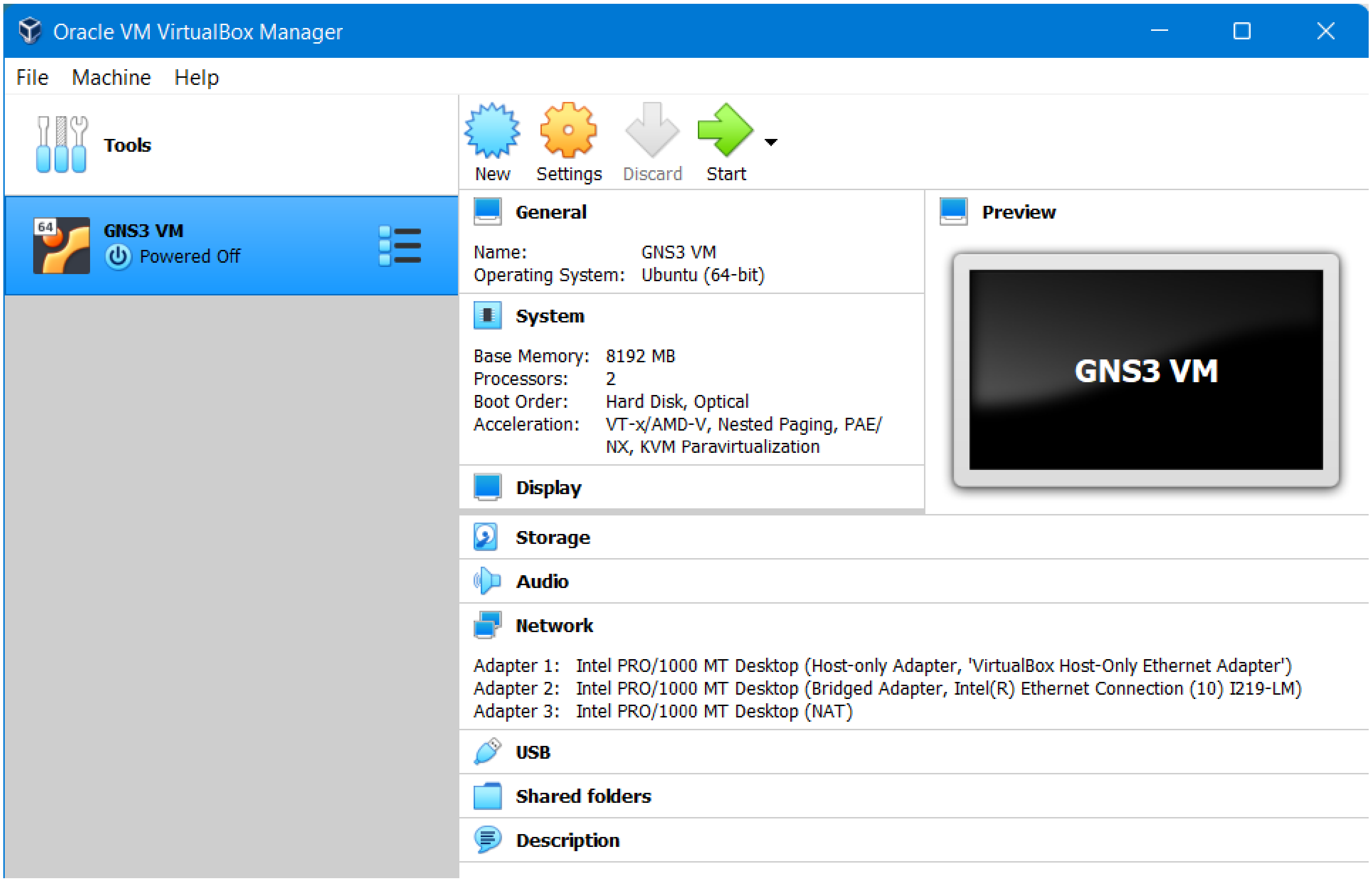
      (4) Select the "Advanced" dropdown

         (a) Promiscuous Mode = Allow All

   c) Network >Adapter 3 tab

      (1) tic the "Enable Network Adapter" box

      (2) Attached to = NAT (not NAT Network)



GNS3 VM
Powered Off

General

Name: GNS3 VM
Operating System: Ubuntu (64-bit)

System

Base Memory: 8192 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

Display

Storage

Audio

Network

Adapter 1: Intel PRO/1000 MT Desktop (Host-only Adapter, 'VirtualBox Host-Only Ethernet Adapter')
Adapter 2: Intel PRO/1000 MT Desktop (Bridged Adapter, Intel(R) Ethernet Connection (10) I219-LM)
Adapter 3: Intel PRO/1000 MT Desktop (NAT)

USB

Shared folders

Description

3. Start the GNS3 VM, select “OK”, type “n” to select “Configure network settings”, select “Yes” (server will reboot after viewing or configuring network settings)

a) uncomment all fields starting with "network"

b) edit the eth0 address to be 192.168.56.101

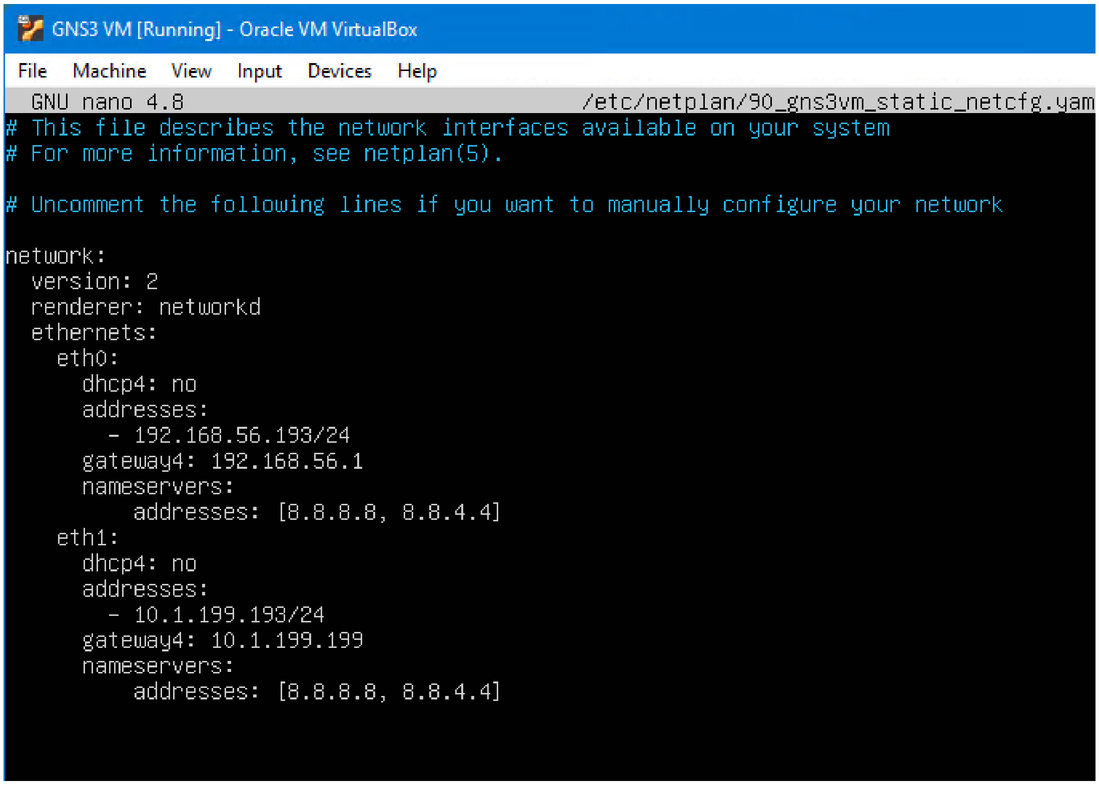
c) edit the eth0 gateway4 to be 192.168.56.1

d) create a new section for eth1, with same entries as eth0, except;

(1) eth1 address to be 10.1.199.101

(2) eth1 gateway to be 10.1.199.199

e) “ctrl+o” to save, “ctrl+x” to exit the editor


GNS3 VM [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

```
  GNU nano 4.8                               /etc/netplan/90_gns3vm_static_netcfg.yam
# This file describes the network interfaces available on your system
# For more information, see netplan(5).

# Uncomment the following lines if you want to manually configure your network

network:
  version: 2
  renderer: networkd
  ethernets:
    eth0:
      dhcp4: no
      addresses:
        - 192.168.56.193/24
      gateway4: 192.168.56.1
      nameservers:
          addresses: [8.8.8.8, 8.8.4.4]
    eth1:
      dhcp4: no
      addresses:
        - 10.1.199.193/24
      gateway4: 10.1.199.199
      nameservers:
          addresses: [8.8.8.8, 8.8.4.4]
```

f) select “OK”, type “s” 4 times to select “Shutdown the VM”, press <enter> to shutdown the VM

V. Install Wireshark

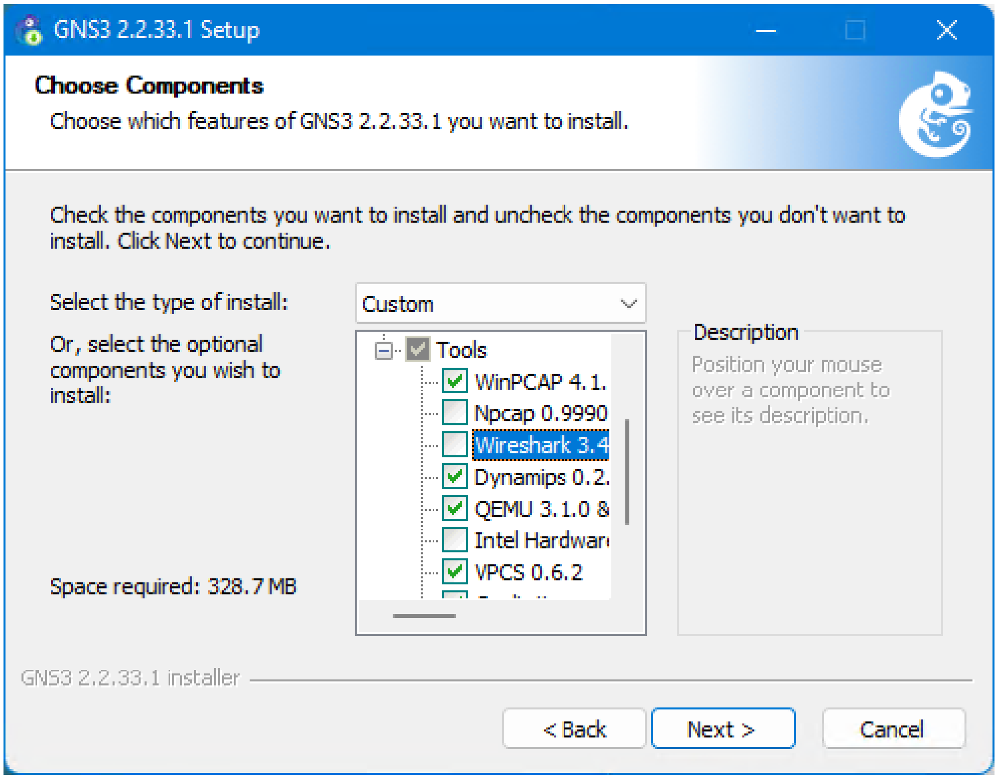
1. Navigate to directory where you copied the Wireshark installer file and install Wireshark (can accept the defaults options during install, or customize for your specific requirements)

VI. Install and configure GNS3

GNS3 was chosen for the network simulation platform as it is a free application, and supports many different host OS's.

1. Navigate to directory where you copied the GNS3 installer file and install GNS3

   a) At the "Choose Components" window, expand the "Tools" section



GNS3 2.2.33.1 Setup

Choose Components

Choose which features of GNS3 2.2.33.1 you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select the type of install: Custom

Or, select the optional components you wish to install:

- ☑ Tools
  - ☑ WinPCAP 4.1.
  - □ Npcap 0.9990
  - □ Wireshark 3.4
  - ☑ Dynamips 0.2.
  - ☑ QEMU 3.1.0 &
  - □ Intel Hardwar
  - ☑ VPCS 0.6.2

Space required: 328.7 MB

Description

Position your mouse over a component to see its description.

GNS3 2.2.33.1 installer

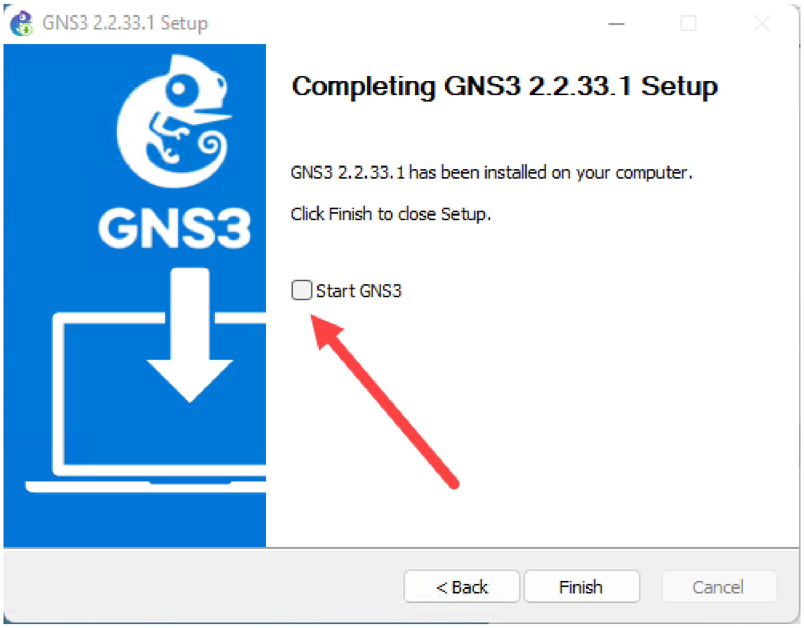
(1) Untic the Npcap 0.9990 box

(2) Untic the Wireshark 3.4.8 box

Note, we want to use the newer versions installed in the previous step

2. At the “Solarwinds Standard Toolset”, select “No”, however if your computer has Internet access, feel free to try the toolset.

3. At the “Completing GNS3 Setup” untic the “Start GNS3” box (ie, do not start GNS3 yet), select finish



Completing GNS3 2.2.33.1 Setup

GNS3 2.2.33.1 has been installed on your computer.

Click Finish to close Setup.

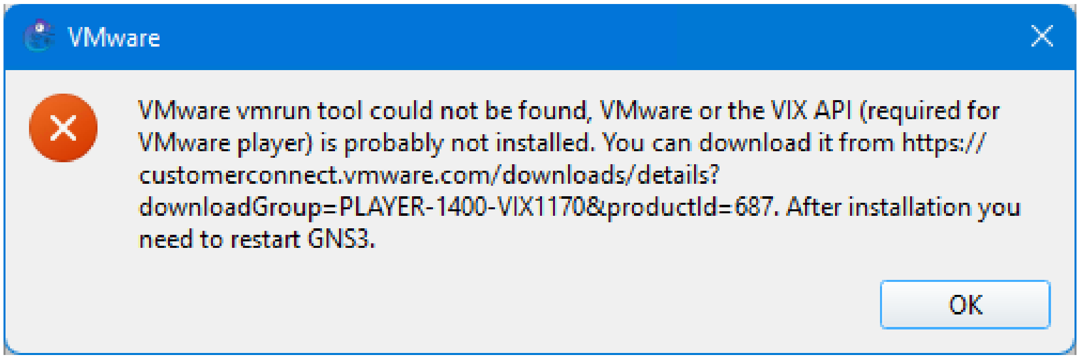
□ Start GNS3

4. Start GNS3

a) at the “Setup Wizard”, select “Run appliances in a virtual machine”

b) click “Next” 3 more times

c) a VMware error box will appear, select “OK” (in this setup option, GNS3 initially attempts to contact the VMware application, as we are using VirtualBox we will select that option in the next step)

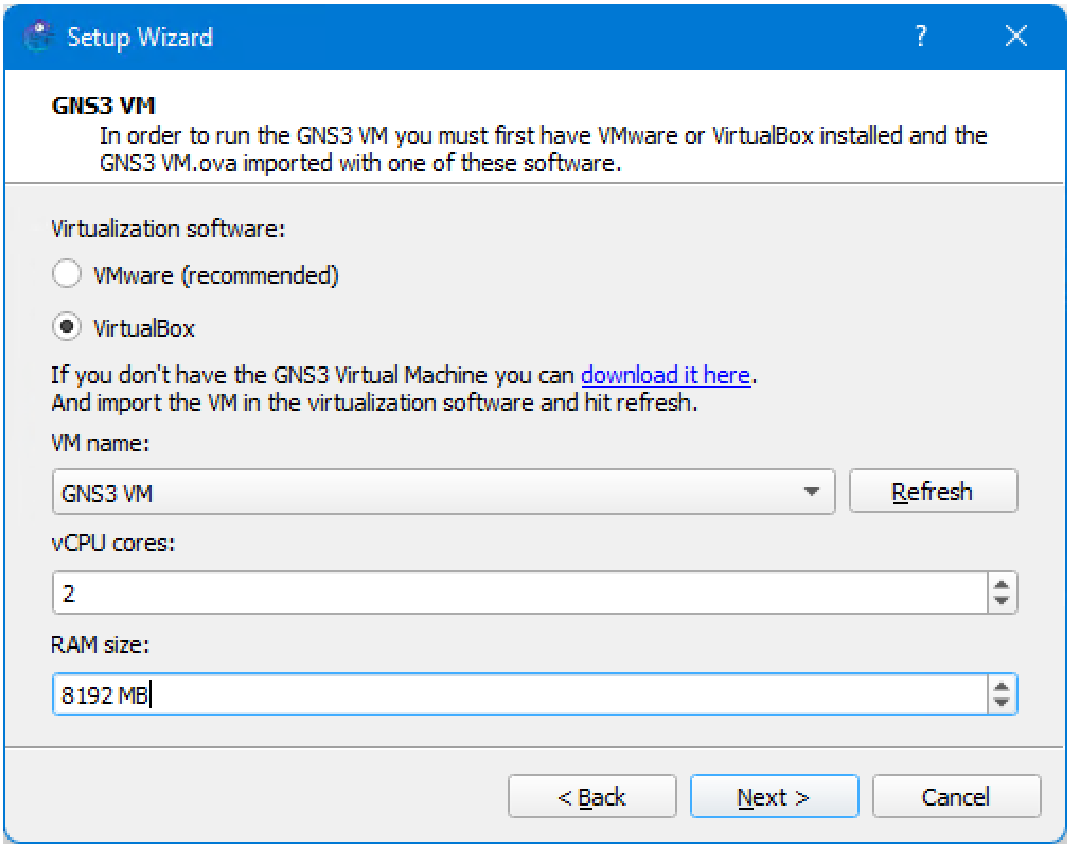


VMware vmrun tool could not be found, VMware or the VIX API (required for VMware player) is probably not installed. You can download it from https://customerconnect.vmware.com/downloads/details?downloadGroup=PLAYER-1400-VIX1170&productId=687. After installation you need to restart GNS3.

d) at GNS3 VM, select “VirtualBox, (GNS3 will then find the VirtualBox-GNS3 VM previously configured)

e) change vCPU cores to 2

f) change RAM size to match your GNS3 VM as configured in VirtualBox



GNS3 VM

In order to run the GNS3 VM you must first have VMware or VirtualBox installed and the GNS3 VM.ova imported with one of these software.

Virtualization software:

○ VMware (recommended)

● VirtualBox

If you don't have the GNS3 Virtual Machine you can download it here.
And import the VM in the virtualization software and hit refresh.

VM name: GNS3 VM

vCPU cores: 2

RAM size: 8192 MB

g) select Next and review the Summary, then select Finish

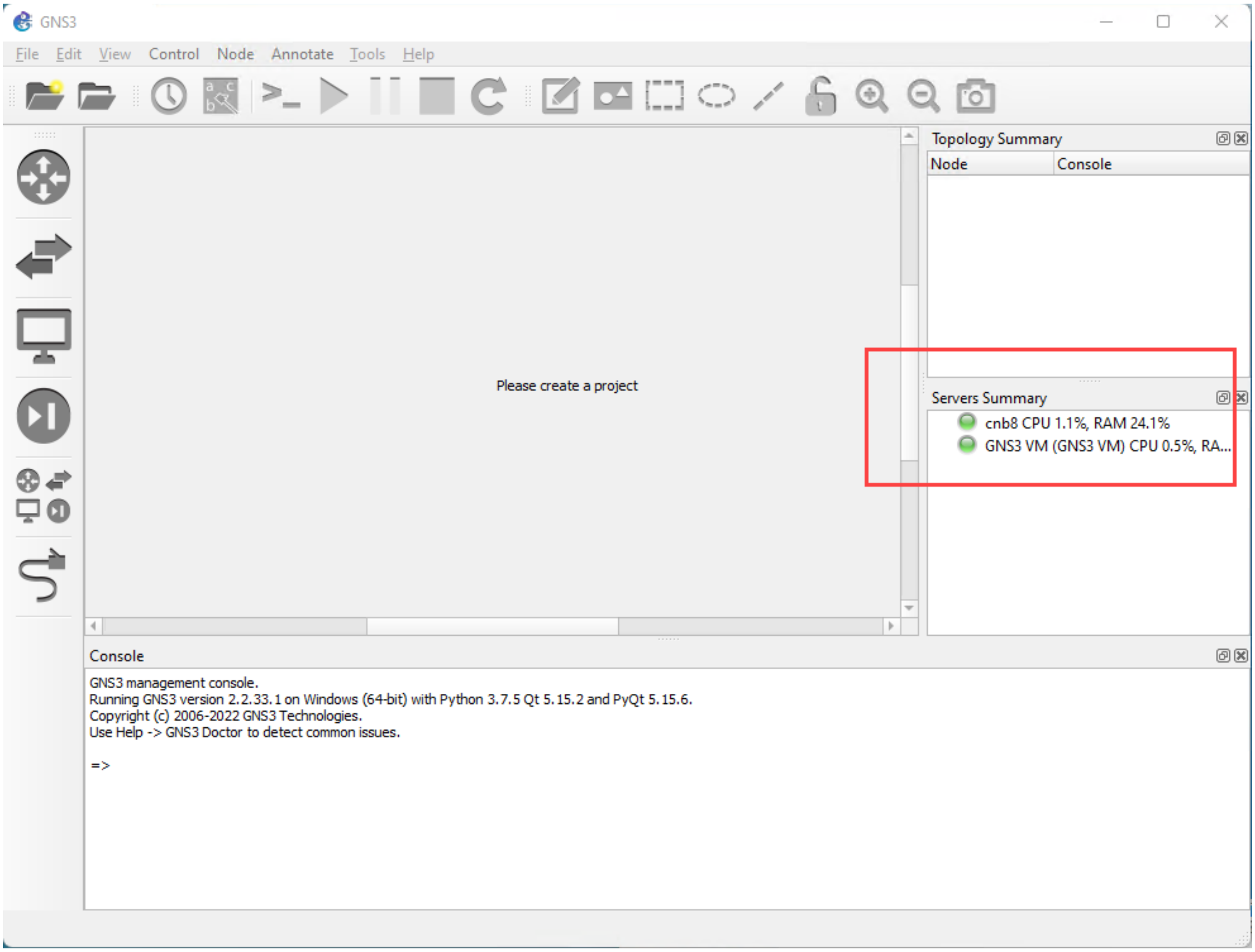
h) quit GNS3

5. After installing/configuring GNS3, navigate to /<user>/GNS3/symbols folder, copy the "vyos.svg" file from the directory where you copied the lab files

6. navigate to /<user>/GNS3/images, copy the "vyos-1.1.8-amd64.iso", "vyos-1.1.8-amd64.iso.md5sum", and "empty8G.qcow2" files from the directory where you copied the lab files

7. Start GNS3

8. After a few minutes, after GNS3 loads, connects to its local server, runs VirtualBox and starts the GNS3 VM, select cancel on the Projects screen, in the Servers Summary pane (middle right side of GNS3) you should observe the local computer and GNS3 VM icons are green



Please create a project

● cnb8 CPU 1.1%, RAM 24.1%
● GNS3 VM (GNS3 VM) CPU 0.5%, RA...

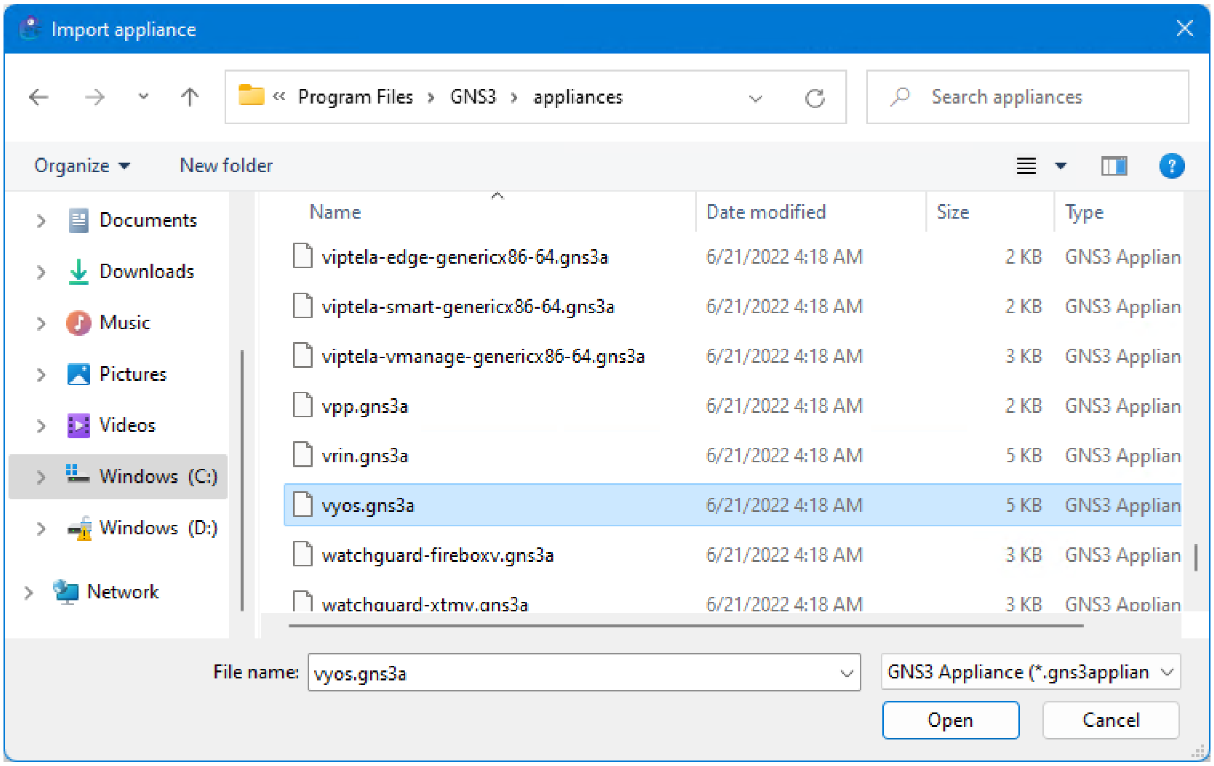
```
GNS3 management console.
Running GNS3 version 2.2.33.1 on Windows (64-bit) with Python 3.7.5 Qt 5.15.2 and PyQt 5.15.6.
Copyright (c) 2006-2022 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=>
```

9. Import the VyOS appliance

a) >File >Import appliance

b) Navigate to C:\Program Files\GNS3\appliances, select vyos.gns3a, select Open



Name	Date modified	Size	Type
viptela-edge-genericx86-64.gns3a	6/21/2022 4:18 AM	2 KB	GNS3 Applian
viptela-smart-genericx86-64.gns3a	6/21/2022 4:18 AM	2 KB	GNS3 Applian
viptela-vmanage-genericx86-64.gns3a	6/21/2022 4:18 AM	3 KB	GNS3 Applian
vpp.gns3a	6/21/2022 4:18 AM	2 KB	GNS3 Applian
vrin.gns3a	6/21/2022 4:18 AM	5 KB	GNS3 Applian
vyos.gns3a	6/21/2022 4:18 AM	5 KB	GNS3 Applian
watchguard-fireboxv.gns3a	6/21/2022 4:18 AM	3 KB	GNS3 Applian
watchguard-xtmv.gns3a	6/21/2022 4:18 AM	3 KB	GNS3 Applian

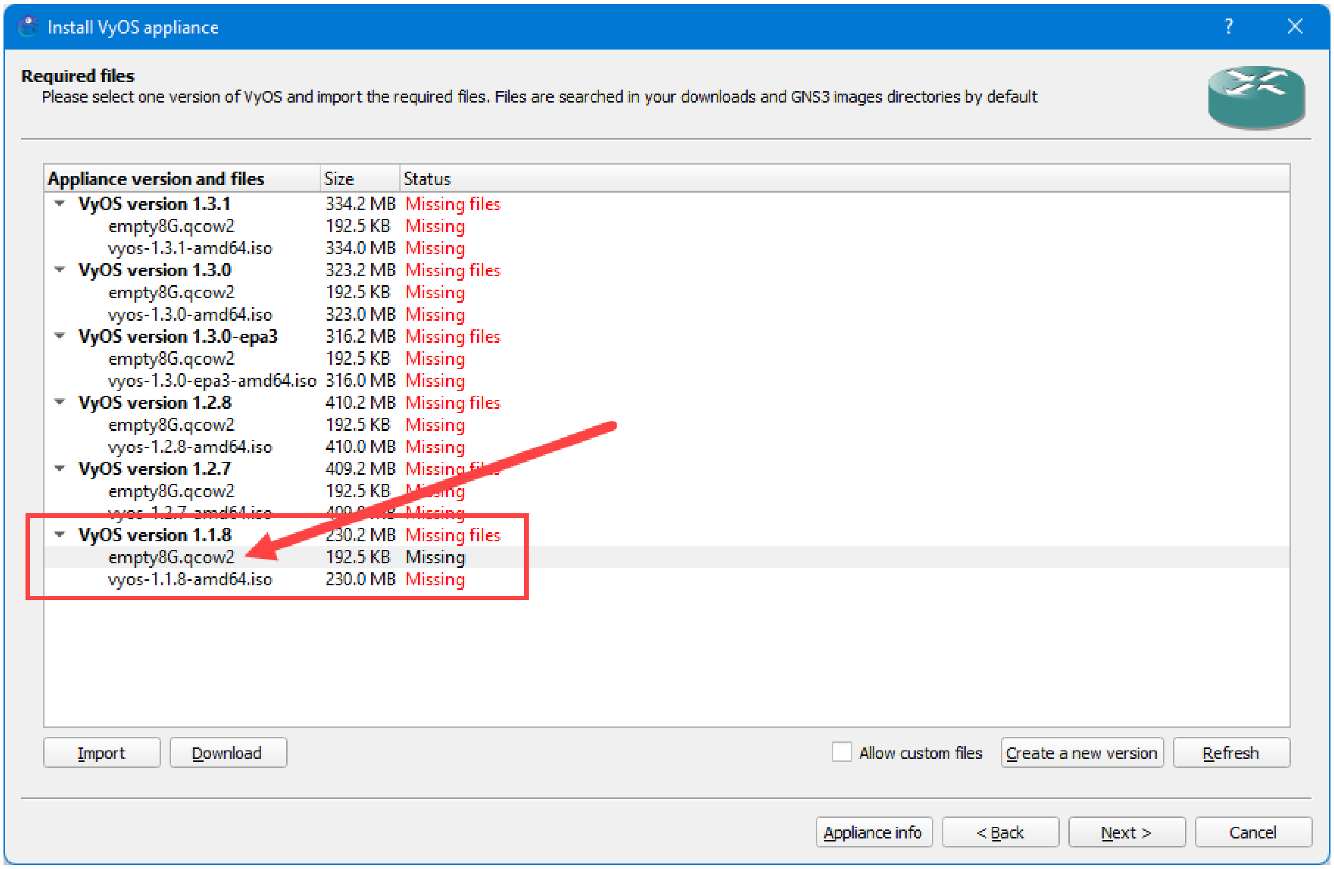
File name: vyos.gns3a

GNS3 Appliance (*.gns3applian

c) Select Next to install the appliance on the GNS3 VM (recommended)”

d) Select Next to use the QEMU settings

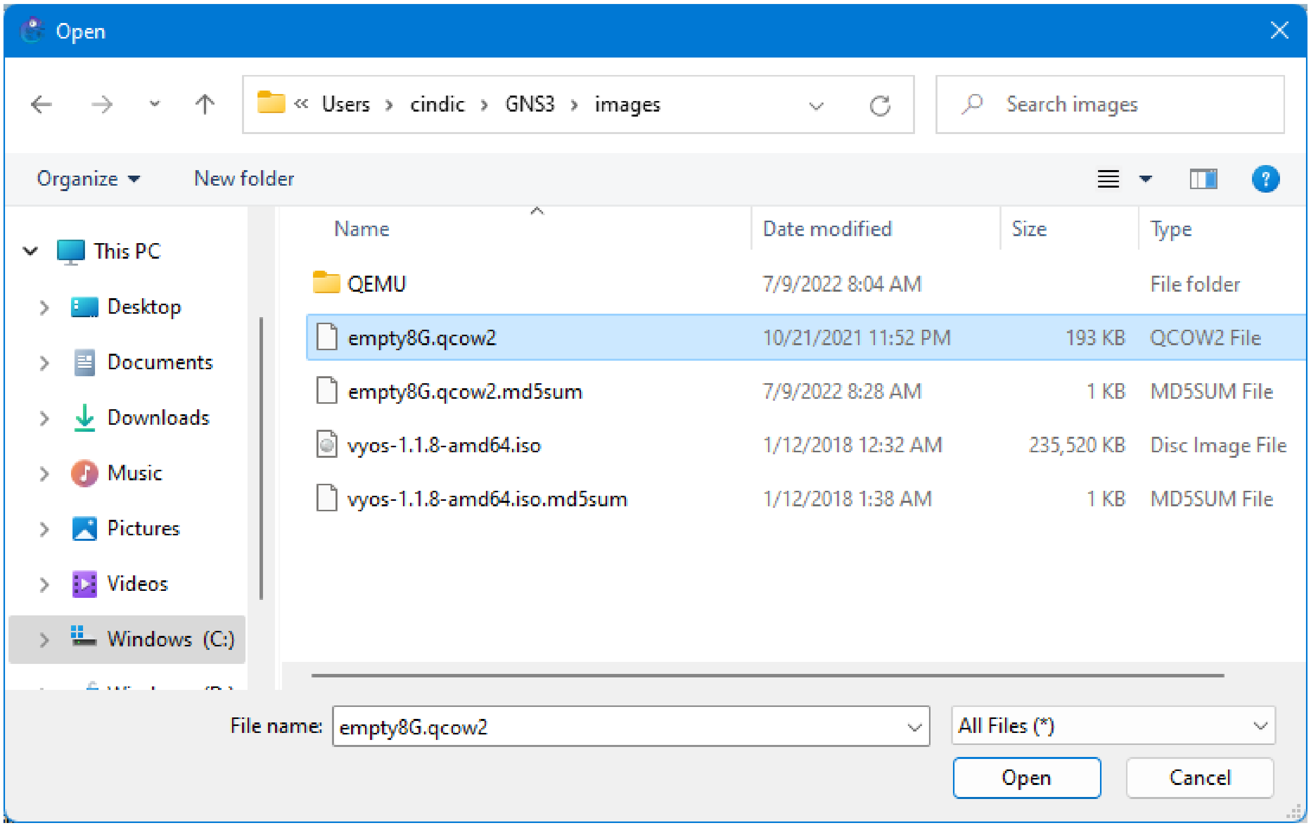
e) at VyOS version 1.1.8, select empty8G.qcow2



Required files
Please select one version of VyOS and import the required files. Files are searched in your downloads and GNS3 images directories by default

Appliance version and files	Size	Status
VyOS version 1.3.1	334.2 MB	Missing files
empty8G.qcow2	192.5 KB	Missing
vyos-1.3.1-amd64.iso	334.0 MB	Missing
VyOS version 1.3.0	323.2 MB	Missing files
empty8G.qcow2	192.5 KB	Missing
vyos-1.3.0-amd64.iso	323.0 MB	Missing
VyOS version 1.3.0-epa3	316.2 MB	Missing files
empty8G.qcow2	192.5 KB	Missing
vyos-1.3.0-epa3-amd64.iso	316.0 MB	Missing
VyOS version 1.2.8	410.2 MB	Missing files
empty8G.qcow2	192.5 KB	Missing
vyos-1.2.8-amd64.iso	410.0 MB	Missing
VyOS version 1.2.7	409.2 MB	Missing files
empty8G.qcow2	192.5 KB	Missing
vyos-1.2.7-amd64.iso	409.0 MB	Missing
VyOS version 1.1.8	230.2 MB	Missing files
empty8G.qcow2	192.5 KB	Missing
vyos-1.1.8-amd64.iso	230.0 MB	Missing

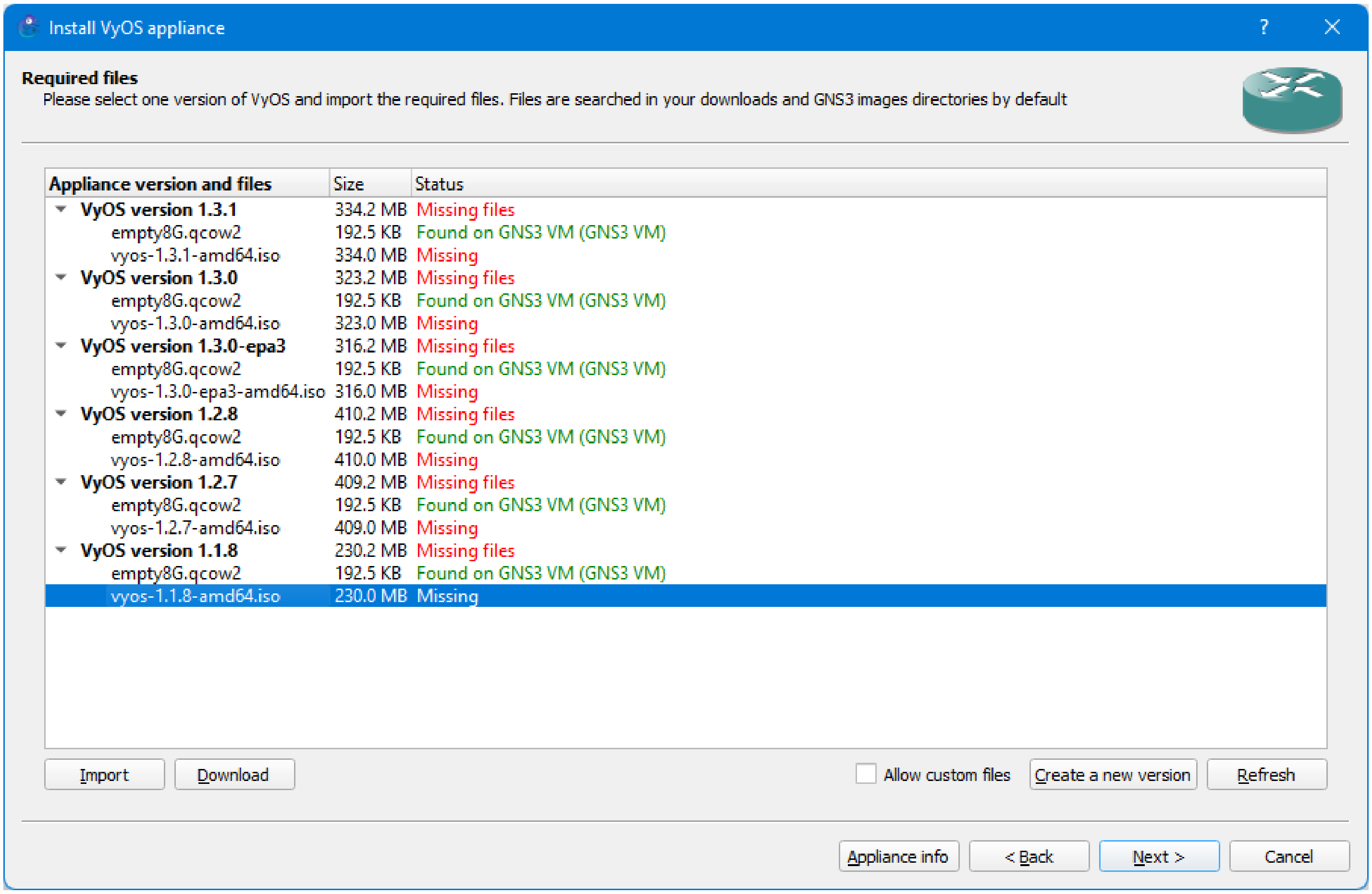
f) select Import, then navigate to /<user>/GNS3/images, select "empty8G.qcow2", select Open



Name	Date modified	Size	Type
QEMU	7/9/2022 8:04 AM		File folder
empty8G.qcow2	10/21/2021 11:52 PM	193 KB	QCOW2 File
empty8G.qcow2.md5sum	7/9/2022 8:28 AM	1 KB	MD5SUM File
vyos-1.1.8-amd64.iso	1/12/2018 12:32 AM	235,520 KB	Disc Image File
vyos-1.1.8-amd64.iso.md5sum	1/12/2018 1:38 AM	1 KB	MD5SUM File

File name: empty8G.qcow2
All Files (*)

g) at VyOS version 1.1.8, select vyos-1.1.8-amd64.iso, then select Import

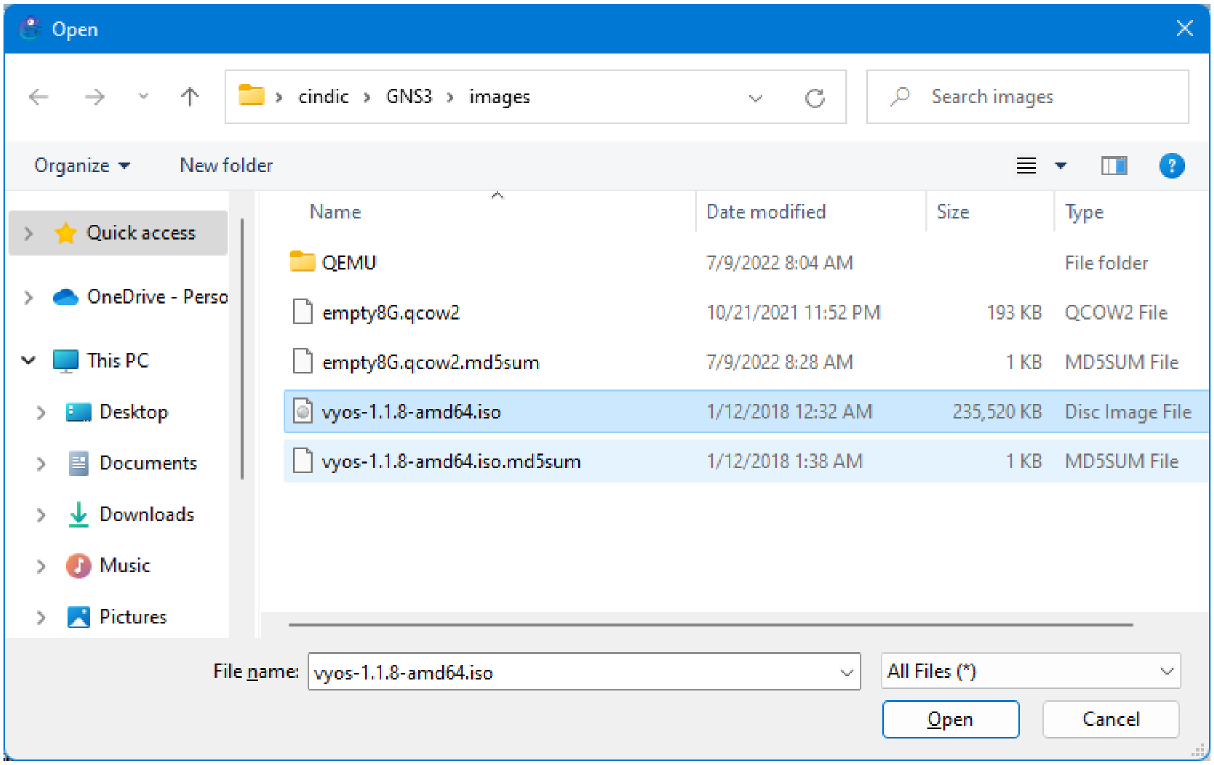


Required files

Please select one version of VyOS and import the required files. Files are searched in your downloads and GNS3 images directories by default

Appliance version and files	Size	Status
VyOS version 1.3.1	334.2 MB	Missing files
empty8G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)
vyos-1.3.1-amd64.iso	334.0 MB	Missing
VyOS version 1.3.0	323.2 MB	Missing files
empty8G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)
vyos-1.3.0-amd64.iso	323.0 MB	Missing
VyOS version 1.3.0-epa3	316.2 MB	Missing files
empty8G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)
vyos-1.3.0-epa3-amd64.iso	316.0 MB	Missing
VyOS version 1.2.8	410.2 MB	Missing files
empty8G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)
vyos-1.2.8-amd64.iso	410.0 MB	Missing
VyOS version 1.2.7	409.2 MB	Missing files
empty8G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)
vyos-1.2.7-amd64.iso	409.0 MB	Missing
VyOS version 1.1.8	230.2 MB	Missing files
empty8G.qcow2	192.5 KB	Found on GNS3 VM (GNS3 VM)
vyos-1.1.8-amd64.iso	230.0 MB	Missing

a) select Import, then navigate to /<user>/GNS3/images, select “empty8G.qcow2”, select Open

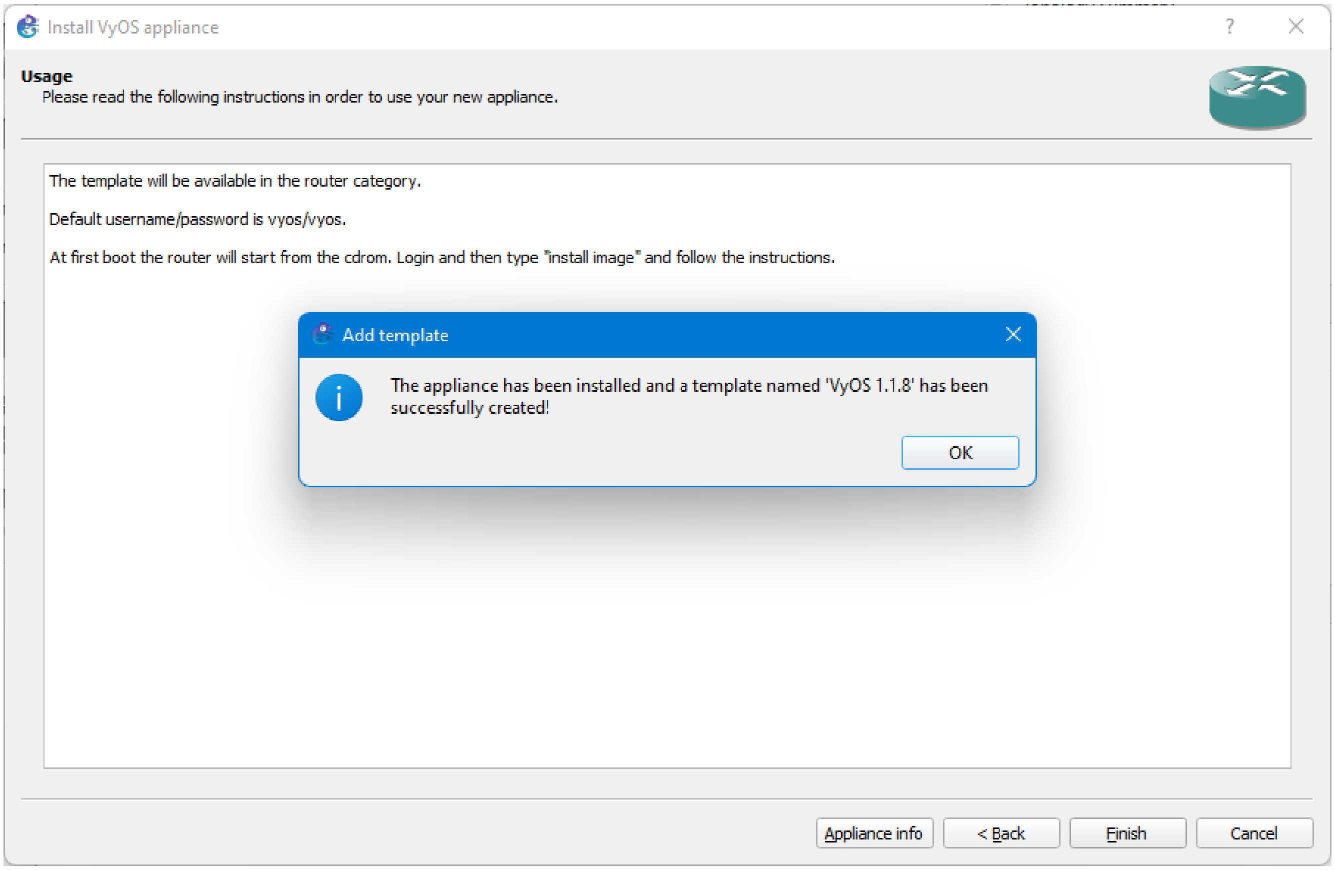


Name	Date modified	Size	Type
QEMU	7/9/2022 8:04 AM		File folder
empty8G.qcow2	10/21/2021 11:52 PM	193 KB	QCOW2 File
empty8G.qcow2.md5sum	7/9/2022 8:28 AM	1 KB	MD5SUM File
vyos-1.1.8-amd64.iso	1/12/2018 12:32 AM	235,520 KB	Disc Image File
vyos-1.1.8-amd64.iso.md5sum	1/12/2018 1:38 AM	1 KB	MD5SUM File

File name: vyos-1.1.8-amd64.iso

b) select VyOS version 1.1.8, select Next to install the VyOS appliance, select Yes to install the appliance, select finish

c) observe the appliance info box and in the foreground window the appliance was installed



Install VyOS appliance
Usage
Please read the following instructions in order to use your new appliance.
Add template
OK
Appliance info
< Back
Finish
Cancel

The template will be available in the router category.

Default username/password is vyos/vyos.

At first boot the router will start from the cdrom. Login and then type "install image" and follow the instructions.

The appliance has been installed and a template named 'VyOS 1.1.8' has been successfully created!

d) select OK

VII. Create Wireshark BYOL project, add VyOS VM

VyOS is used to for many operations in this lab system. It is the router between the multiple networks you will be configuring and also SSH/Telnet/SNMP/DHCP/DHCPv6 services.

1. In GNS3,>File >New blank project

    a) Set Name to be Wireshark-BYOL, select "OK"

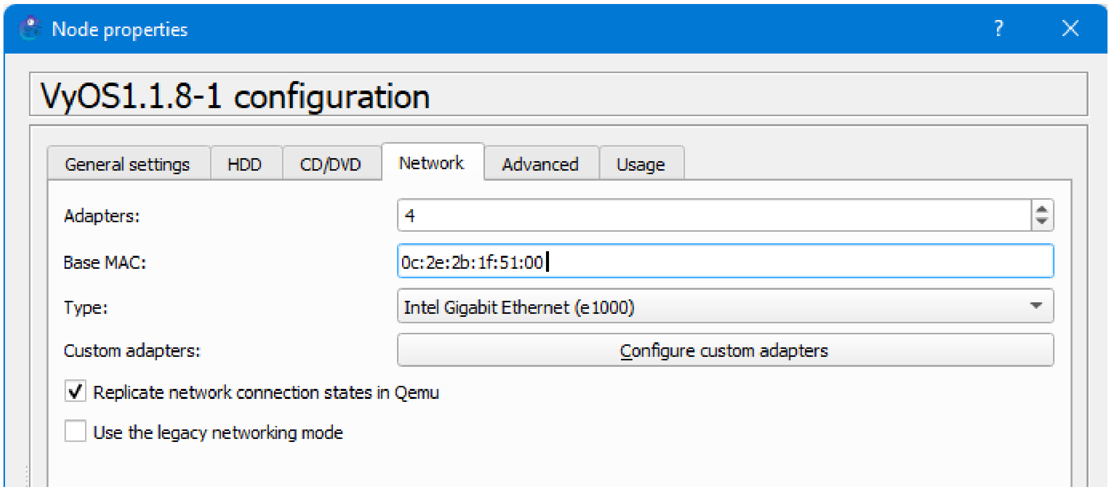
2. In the Wireshark-BYOL – GNS3 window, select the "Browse Routers" icon in the left-side navigation

3. Click and drag the VyOS1.1.8-1 icon to the middle of the projects main screen, click the "Browse Routers" icon again to close the window

4. Configure the VyOS VM: right-click the VyOS icon, select Configure, select the "Network" tab

    a) set Adapters to 4

    b) set Base MAC to 0c:2e:2b:1f:01:00



Adapters: 4

Base MAC: 0c:2e:2b:1f:51:00

Type: Intel Gigabit Ethernet (e1000)

Custom adapters:

☑ Replicate network connection states in Qemu

☐ Use the legacy networking mode

    c) click "OK"

5. Start VyOS: right-click to VyOS icon, select Start, then right-click the VyOS icon and select Console (a PuTTY session will popup for the console access)

6. Log into VyOS using vyos and vyos

7. Install the VyOS Image: type "install image" at the CLI

    a) accept most default settings

    b) at "This will destroy all data on /dev/sda", type "yes"

c) set name to be VyOS-1.1.8-1

d) at “Enter password for user vyos”, enter vyos 2 times

e) enter “poweroff now”, then VM will stop and the console window will close

8. Configure the VyOS VM, right-click the VyOS icon, select Configure, select the “CD/DVD” tab

a) Clear the Image field (ie, remove the iso filename)

b) click “OK”

VIII. Configure VyOS

The overall process to configure VyOS as an IPv4/IPv6 router and DHCP/DHCPv6 server is very long, with many steps. As you maneuver through this section, go slow and check the commands you have entered closely.

1. In GNS3 UI, right-click the VyOS router icon, select the "Start" button to load the VyOS-router VM

2. In GNS3 UI, right-click the VyOS router icon, select the "Console" button to open a terminal session to the VyOS router

3. In the terminal session for the VyOS router, login: login as "vyos", password is "vyos"

4. Navigate to the configuration mode

    a) configure

5. configure host name

    a) set system host-name VyOS-1.1.8-1

6. configure SSH access

    a) set service ssh port 22

    b) set service ssh allow-root

7. configure Telnet access

    a) set service telnet port 23

    b) set service telnet allow-root

8. configure IPv4 and IPv6 name servers

    a) set system name-server 192.168.101.53

    b) set system name-server 200:61ab:101:1681::53

9. configure SNMP

    a) set service snmp community private authorization rw

    b) set service snmp community public authorization ro

    c) set service snmp contact lab-NOC

    d) set service snmp description VyOS-1.1.8-1

    e) set service snmp location GNS3-VM

    f) set service snmp trap-target 192.168.101.53

10. configure timezone

    a) set system time-zone America/Chicago

        (1) (to select your specific time zone, type 'set system time-zone ?" to find Region, type in your region, then add '?' to find city.)

    b) commit

    c) save

11. Configuring IPv4 and IPv6 addresses, and RA for no-advertise on the eth0 interface

    a) set interfaces ethernet eth0 address 10.1.199.201/24

    b) set interfaces ethernet eth0 address 200:61ab:199:1011::201/64

    c) set interfaces ethernet eth0 ipv6 router-advert max-interval 180

    d) set interfaces ethernet eth0 ipv6 router-advert min-interval 60

    e) set interfaces ethernet eth0 ipv6 router-advert managed-flag false

    f) set interfaces ethernet eth0 ipv6 router-advert other-config-flag false

    g) set interfaces ethernet eth0 ipv6 router-advert default-lifetime 1800

    h) set interfaces ethernet eth0 ipv6 router-advert send-advert false

    i) set interfaces ethernet eth0 ipv6 router-advert prefix 200:61ab:199:1011::/64

    j) set interfaces ethernet eth0 ipv6 router-advert prefix 200:61ab:199:1011::/64 autonomous-flag true

    k) set interfaces ethernet eth0 ipv6 router-advert prefix 200:61ab:199:1011::/64 on-link-flag true

    l) set interfaces ethernet eth0 ipv6 router-advert prefix 200:61ab:199:1011::/64 preferred-lifetime 120

    m) set interfaces ethernet eth0 ipv6 router-advert prefix 200:61ab:199:1011::/64 valid-lifetime 140

    n) commit

    o) save

12. Configuring IPv4 and IPv6 addresses, and RA for SLAAC advertise on the eth1 interface

    a) set interfaces ethernet eth1 address 172.20.01.1/24

    b) set interfaces ethernet eth1 address 200:61ab:01:201::1/64

c) set interfaces ethernet eth1 ipv6 router-advert max-interval 180

d) set interfaces ethernet eth1 ipv6 router-advert min-interval 60

e) set interfaces ethernet eth1 ipv6 router-advert managed-flag false

f) set interfaces ethernet eth1 ipv6 router-advert other-config-flag false

g) set interfaces ethernet eth1 ipv6 router-advert default-lifetime 1800

h) set interfaces ethernet eth1 ipv6 router-advert send-advert true

i) set interfaces ethernet eth1 ipv6 router-advert prefix 200:61ab:01:201::/64

j) set interfaces ethernet eth1 ipv6 router-advert prefix 200:61ab:01:201::/64 autonomous-flag true

k) set interfaces ethernet eth1 ipv6 router-advert prefix 200:61ab:01:201::/64 on-link-flag true

l) set interfaces ethernet eth1 ipv6 router-advert prefix 200:61ab:01:201::/64 preferred-lifetime 120

m) set interfaces ethernet eth1 ipv6 router-advert prefix 200:61ab:01:201::/64 valid-lifetime 140

n) commit

o) save

13. Configuring IPv4 and IPv6 addresses and RA for Stateful DHCPv6 advertise on the eth2 interface

a) set interfaces ethernet eth2 address 10.10.01.1/24

b) set interfaces ethernet eth2 address 200:61ab:01:1010::1/64

c) set interfaces ethernet eth2 ipv6 router-advert max-interval 180

d) set interfaces ethernet eth2 ipv6 router-advert min-interval 60

e) set interfaces ethernet eth2 ipv6 router-advert managed-flag true

f) set interfaces ethernet eth2 ipv6 router-advert other-config-flag false

g) set interfaces ethernet eth2 ipv6 router-advert default-lifetime 1800

h) set interfaces ethernet eth2 ipv6 router-advert send-advert true

i) set interfaces ethernet eth2 ipv6 router-advert prefix 200:61ab:01:1010::/64

j) set interfaces ethernet eth2 ipv6 router-advert prefix 200:61ab:01:1010::/64 autonomous-flag false

k) set interfaces ethernet eth2 ipv6 router-advert prefix 200:61ab:01:1010::/64 on-link-flag true

l) set interfaces ethernet eth2 ipv6 router-advert prefix 200:61ab:01:1010::/64 preferred-lifetime 120

m) set interfaces ethernet eth2 ipv6 router-advert prefix 200:61ab:01:1010::/64 valid-lifetime 140

n) commit

o) save

14. Configuring IPv4 and IPv6 addresses, and RA for SLAAC advertise on the eth3 interface

a) set interfaces ethernet eth3 address 192.168.01.1/24

b) set interfaces ethernet eth3 address 200:61ab:01:1681::f254/64

c) set interfaces ethernet eth3 ipv6 router-advert max-interval 180

d) set interfaces ethernet eth3 ipv6 router-advert min-interval 60

e) set interfaces ethernet eth3 ipv6 router-advert managed-flag false

f) set interfaces ethernet eth3 ipv6 router-advert other-config-flag false

g) set interfaces ethernet eth3 ipv6 router-advert default-lifetime 1800

h) set interfaces ethernet eth3 ipv6 router-advert send-advert true

i) set interfaces ethernet eth3 ipv6 router-advert prefix 200:61ab:01:1681::/64

j) set interfaces ethernet eth3 ipv6 router-advert prefix 200:61ab:01:1681::/64 autonomous-flag true

k) set interfaces ethernet eth3 ipv6 router-advert prefix 200:61ab:01:1681::/64 on-link-flag true

l) set interfaces ethernet eth3 ipv6 router-advert prefix 200:61ab:01:1681::/64 preferred-lifetime 120

m) set interfaces ethernet eth3 ipv6 router-advert prefix 200:61ab:01:1681::/64 valid-lifetime 140

n) commit

o) save

15. Configuring DHCPv6 Service for the eth2 interface

a) set service dhcpv6-server shared-network-name eth2 subnet 200:61ab:01:1010::/64 address-range start 200:61ab:01:1010::101 stop 200:61ab:01:1010::119

b) set service dhcpv6-server shared-network-name eth2 subnet 200:61ab:01:1010::/64 lease-time default 300

c) set service dhcpv6-server shared-network-name eth2 subnet 200:61ab:01:1010::/64 lease-time maximum 300

d) set service dhcpv6-server shared-network-name eth2 subnet 200:61ab:01:1010::/64 lease-time minimum 225

e) set service dhcpv6-server shared-network-name eth2 subnet 200:61ab:01:1010::/64 name-server 200:61ab:01:1681::53

f) commit

g) save

16. Configuring DHCP Service for the eth1 interface

a) set service dhcp-server shared-network-name eth1 subnet 172.20.01.0/24 default-router 172.20.01.1

b) set service dhcp-server shared-network-name eth1 subnet 172.20.01.0/24 dns-server 192.168.01.53

c) set service dhcp-server shared-network-name eth1 subnet 172.20.01.0/24 lease 300

d) set service dhcp-server shared-network-name eth1 subnet 172.20.01.0/24 start 172.20.01.102 stop 172.20.01.119

e) commit

f) save

17. Configuring DHCP Service for the eth2 interface

a) set service dhcp-server shared-network-name eth2 subnet 10.10.01.0/24 default-router 10.10.01.1

b) set service dhcp-server shared-network-name eth2 subnet 10.10.01.0/24 dns-server 192.168.01.53

c) set service dhcp-server shared-network-name eth2 subnet 10.10.01.0/24 lease 300

d) set service dhcp-server shared-network-name eth2 subnet 10.10.01.0/24 start 10.10.01.102 stop 10.10.01.119

e) commit

f) save

18. Configuring DHCP Service for the eth3 interface

a) set service dhcp-server shared-network-name eth3 subnet 192.168.01.0/24 default-router 192.168.01.1

b) set service dhcp-server shared-network-name eth3 subnet 192.168.1.0/24 dns-server 192.168.01.53

c) set service dhcp-server shared-network-name eth3 subnet 192.168.1.0/24 lease 300

d) set service dhcp-server shared-network-name eth3 subnet 192.168.1.0/24 start 192.168.1.101 stop 192.168.1.119

e) commit

f) save

19. Configuring IPv6 default route for workshop core

a) set protocols static route6 0::/0 next-hop fe80::20c:29ff:fe17:957b interface eth0

b) commit

c) save

d) exit

IX. Configuring the Wireshark-BYOL project, add the host and Switches

1. In the Wireshark-BYOL – GNS3 window, select the “Browse End Devices” icon in the left-side navigation

2. Click and drag the Cloud icon to the middle of the projects main screen, above the VyOS icon

    a) choose “GNS3 VM” as the Server, select OK

    b) click the “Browse End Devices” icon again to close the window

3. Configure the Cloud resource: right-click the Cloud icon, select Change hostname

    a) set Hostname to be name of host computer

4. Configure the Cloud resource: right-click the Cloud icon, select Change symbol

    a) expand “Affinity-square-blue

    b) select the “client” icon

    c) select “OK”

5. Align icons as needed

6. Connect the VyOS router to the host

    a) click the “Add a link” icon in the left-side navigation

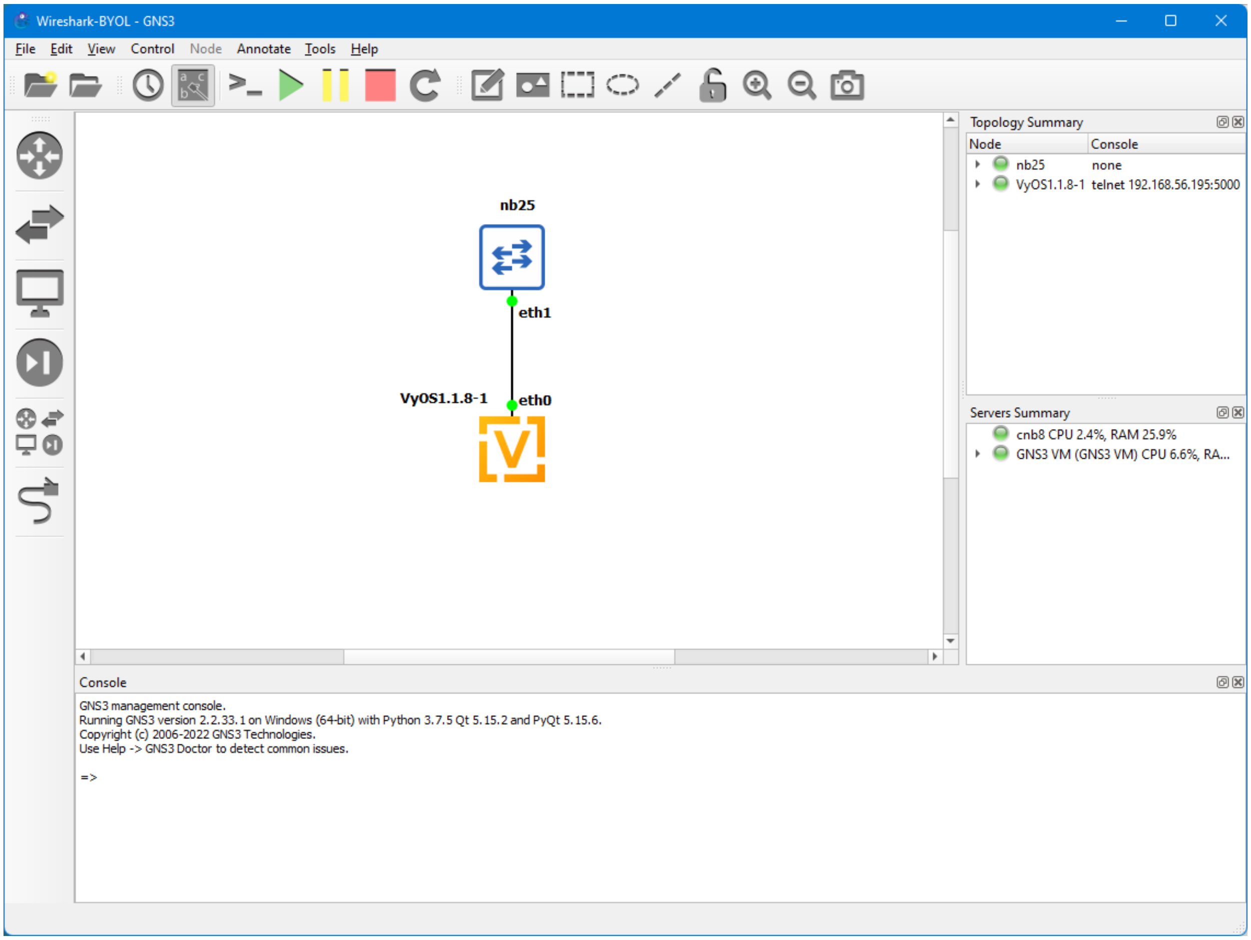
    b) select the host icon, select eth1

    c) select the VyOS icon, select eth0

    d) click the “Add a link” icon again to exit adding links

7. On the GNS3 toolbar, select the “Show/Hide interface labels” icon (this will show the interfaces that have connections in the project)

8. Adjust labels/icons as needed for viewing clarity



Topology Summary

Node	Console
nb25	none
VyOS1.1.8-1	telnet 192.168.56.195:5000

Servers Summary

cnb8 CPU 2.4%, RAM 25.9%

GNS3 VM (GNS3 VM) CPU 6.6%, RA...

Console

```
GNS3 management console.
Running GNS3 version 2.2.33.1 on Windows (64-bit) with Python 3.7.5 Qt 5.15.2 and PyQt 5.15.6.
Copyright (c) 2006-2022 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=>
```

9. In the VyOS console window, ping the host (if the host has an address in the 10.1.199.0/24 network)

10. In the Wireshark-BYOL – GNS3 window, select the “Browse Switches” icon in the left-side navigation

11. Click and drag the Ethernet switch icon to the left of the VyOS icon

    a) choose “GNS3 VM” as the Server, select OK

12. Click and drag the Ethernet switch icon to the right of the VyOS icon

    a) choose “GNS3 VM” as the Server, select OK

13. Click and drag the Ethernet switch icon to the bottom of the VyOS icon

    a) choose “GNS3 VM” as the Server, select OK

    b) click the “Browse Switches” icon again to close the window

14. Configure each of the Switch resources: right-click each of the the Switch icons, select Change symbol

    a) expand “Affinity-square-blue

    b) select the “switch” icon

    c) select “OK”

15. Align icons as needed

16. Connect the VyOS router to each switch

    a) click the “Add a link” icon in the left-side navigation

    b) select the Switch1 icon, select eth0

    c) select the VyOS icon, select eth1

    d) select the Switch2 icon, select eth0

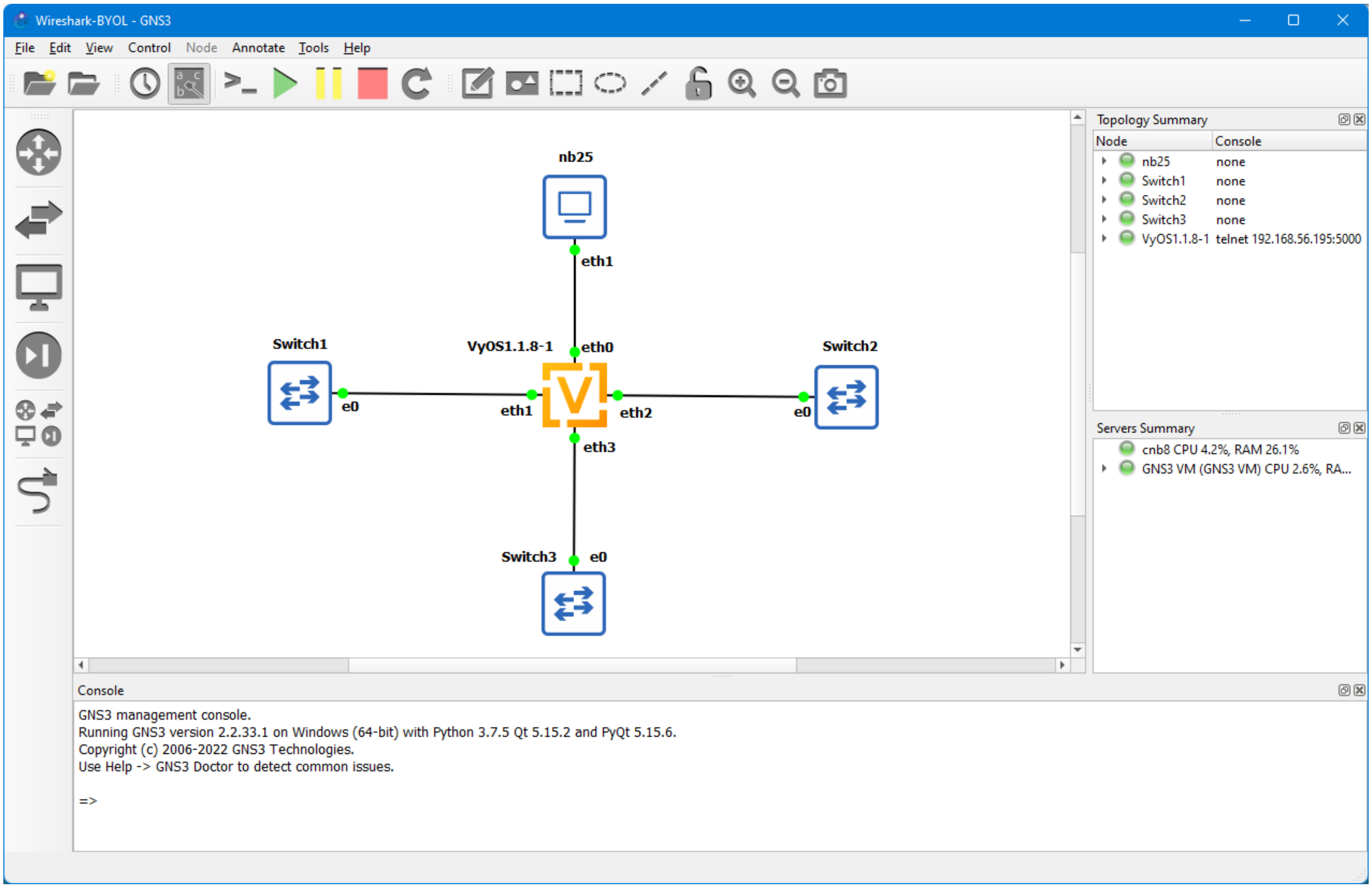
    e) select the VyOS icon, select eth2

    f) select the Switch3 icon, select eth0

    g) select the VyOS icon, select eth3

    h) click the “Add a link” icon again to exit adding links

17. Adjust labels/icons as needed for viewing clarity)



Node	Console
nb25	none
Switch1	none
Switch2	none
Switch3	none
VyOS1.1.8-1	telnet 192.168.56.195:5000

cnb8 CPU 4.2%, RAM 26.1%

GNS3 VM (GNS3 VM) CPU 2.6%, RA...

```
GNS3 management console.
Running GNS3 version 2.2.33.1 on Windows (64-bit) with Python 3.7.5 Qt 5.15.2 and PyQt 5.15.6.
Copyright (c) 2006-2022 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=>
```

X. Create Rocky Linux VM’s

Any Linux distro you would rather use is ok, basic directions to get such into the lab may be similar.

1. In VirtualBox, select "New" to create the new virtual machine

2. Set the "Name" field to “Rocky-8.5-1”, the "Type" field to “Linux”, and the "Version" field to “Other Linux (64 bit)”

3. Configure the "Memory size" setting of 2048MB

4. Verify the "Hard drive" setting is selected for "Create a virtual hard drive now", select Create

5. Configure the "File size" "16.00 GB”

6. Verify the "Hard drive file type" setting is selected for "VDI (VirtualBox Disk Image)"

7. Verify the "Storage on physical hard drive" setting is selected for "Dynamically allocated", select Create

8. You should now see the newly created Rocky-8.5-1 VM in the "Oracle VM VirtualBox Manager" window

9. There are a few changes to be made before running/installing VyOS, select the “Settings” icon for the Rocky VM

    a) Select "Network" on the left side panel. In the Adapter 1 tab, change the "Attached to:" box to "Not attached”

    b) Select "Storage" on the left side panel, in the "Storage Devices" area, click the icon that looks like a CD and is labeled "Empty", then in the "Attributes" area, click the icon that looks like a CD/DVD, select "Choose a virtual CD/DVD disk file", navigate to where the Rocky Linux ISO is located and select Open

    c) Select "Display" on the left side panel. In the change the "Scale Factor:" box dependent on host video resolution, then select “OK”

        (1) FHD 1920 x 1080, leave display set to 100%

        (2) QHD 2560 x 1440, set display to 200%,

        (3) UHD 3840 x 2160, set display to 300%

10. In the "Oracle VM VirtualBox Manager" window, verify the Rocky Linux settings

11. Select the "Start" button to load the Rocky-8.5-1 VM

12. When the Rocky Linux 8 screen is presented, select “Install Rocky Linux 8”, Follow the install prompt to configure and install Rocky Linus

    a) Select your language as appropriate

b) Configure the Root Password" to be "password" (will require 2 Done to confirm)

c) Configure "Time & Date" as appropriate for your timezone

d) Choose "Installation Destination" and then select "Done"

e) Can create a new user if you want, not required

f) Select "Begin Installation" to complete the Rocky Linux installation process, may take 7-10 minutes to complete

g) Select "Reboot System" in the lower-righton the screen

h) At the "INITIAL SETUP" screen, select "LICENSING", tic the "I accept the license agreement" box, select "Done", then select "FINISH CONFIGURATION"

i) At the "Welcome!" screen, select "Next"

j) Configure "Location Services" to "OFF", select Next

k) At the "Online Accounts" screen, select "Skip"

l) At the "About You" screen, configure as appropriate, then select "Start Using Rocky Linux"

13. After the installation process has completed, power down the Rocky-8.5-1 VM

14. Clone the Rocky-8.5-1 VM

a) In the "Oracle VM VirtualBox Manager" window, right-click the Rocky-8.5-1 VM and select "Clone"

b) Set Name: to Rocky-8.5-2, select "Next"

c) Verify the "Full clone" button is selected, select "Clone"

XI. Configuring the Wireshark-BYOL project, add the Rocky VMs

1. Add the Rocky VMs to the project: in the Wireshark-BYOL – GNS3 window, select >Edit >Preferences >VirtualBox VMs

   a) Select New, in "Server" window select "Next", in VirtualBox Virtual Machine select Rocky-8.5-1 then select "Finish"

   b) Select New, in "Server" window select "Next", in VirtualBox Virtual Machine select Rocky-8.5-2 then select "Finish", then select "OK"

2. In the Wireshark-BYOL – GNS3 window, select the "Browse End Devices" icon in the left-side navigation

3. Click and drag the Rocky-8.5-1 icon to the mid-upper-left of the projects main screen, above the left corner of the Switch1 icon

4. Click and drag the Rocky-8.5-2 icon to the mid-upper-right of the projects main screen, above the right corner of the Switch2 icon

   a) click the "Browse End Devices" icon again to close the window

5. Align icons as needed

6. Connect the Rocky VMs to the switch

   a) click the "Add a link" icon in the left-side navigation

   b) select the Rocky-8.5-1-1 icon, select eth0

   c) select the Switch1 icon, select eth1

   d) select the Rocky-8.5-2-1 icon, select eth0

   e) select the Switch2 icon, select eth1

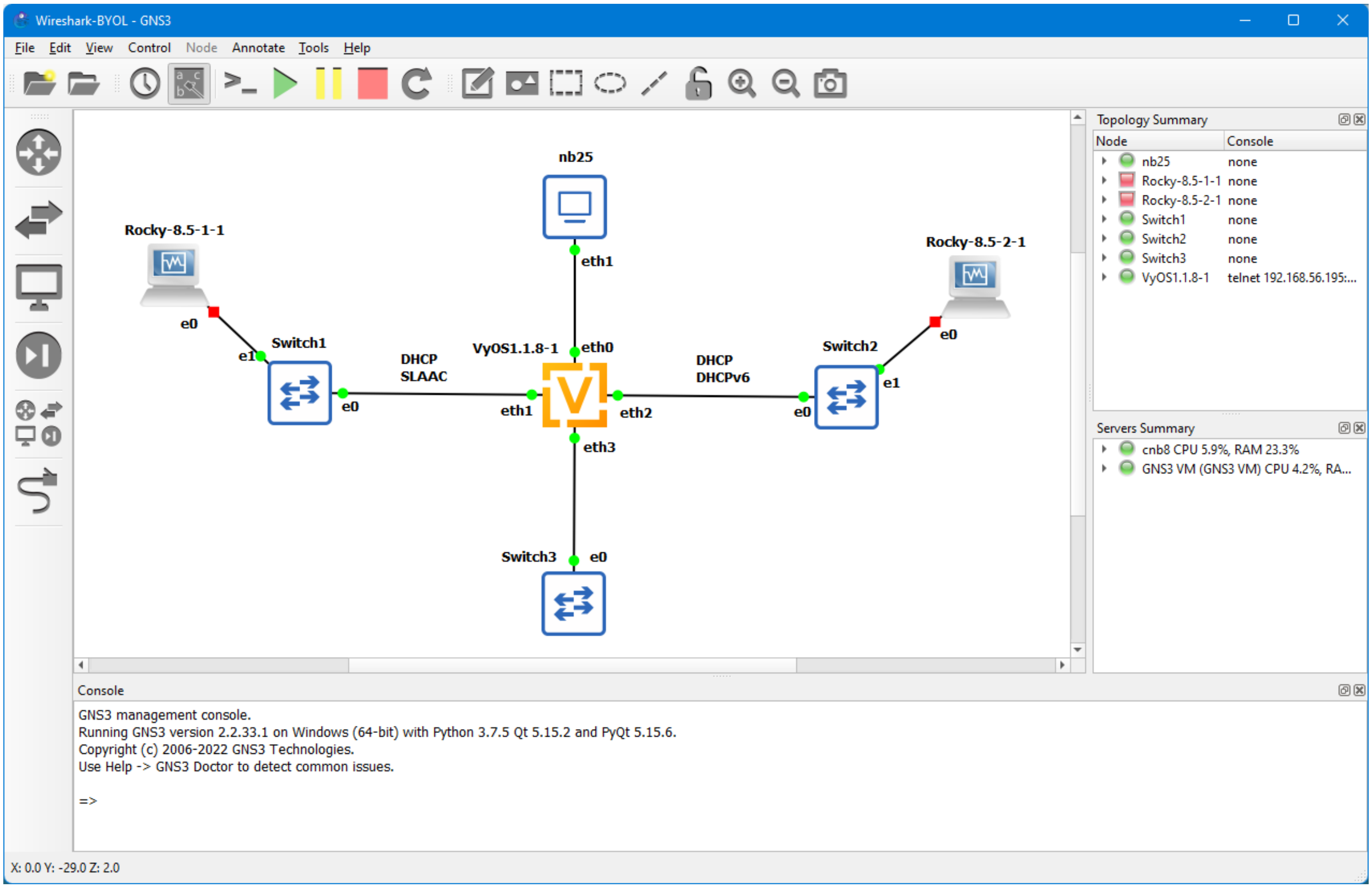
   f) click the "Add a link" icon again to exit adding links

7. Adjust labels/icons as needed for viewing clarity

8. Add text above the VyOS1.1.8-1 and Switch1 link: 2 lines: DHCP and SLAAC, in the Wireshark-BYOL – GNS3 window, select the "Add a note" icon in the top toolbar

9. Add text above the VyOS1.1.8-1 and Switch2 link: 2 lines: DHCP and DHCPv6, in the Wireshark-BYOL – GNS3 window, select the "Add a note" icon in the top toolbar

10. Adjust labels/icons as needed for viewing clarity



Node	Console
nb25	none
Rocky-8.5-1-1	none
Rocky-8.5-2-1	none
Switch1	none
Switch2	none
Switch3	none
VyOS1.1.8-1	telnet 192.168.56.195:...

cnb8 CPU 5.9%, RAM 23.3%
GNS3 VM (GNS3 VM) CPU 4.2%, RA...

```
GNS3 management console.
Running GNS3 version 2.2.33.1 on Windows (64-bit) with Python 3.7.5 Qt 5.15.2 and PyQt 5.15.6.
Copyright (c) 2006-2022 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=>
```

XII. Create Windows 10 VM’s

If you only have 8GB RAM in your host computer, you may not want to attempt Windows VMs, as there may not be enough resources in the host.

1. In VirtualBox, select "New" to create the new virtual machine

2. Set the "Name" field to “Win10-Ent-1” and the "Version" field to “Windows 10 (64 bit)”

3. Verify the "Memory size" setting of 2048MB

4. Verify the "Hard drive" setting is selected for "Create a virtual hard drive now", select Create

5. Configure the "File size" "20.00 GB”

6. Verify the "Hard drive file type" setting is selected for "VDI (VirtualBox Disk Image)"

7. Verify the "Storage on physical hard drive" setting is selected for "Dynamically allocated", select Create

8. You should now see the newly created Win10-Ent-1 VM in the "Oracle VM VirtualBox Manager" window

9. There are a few changes to be made before running/installing VyOS, select the “Settings” icon for the Windows VM

    a) Select "Network" on the left side panel. In the Adapter 1 tab, change the "Attached to:" box to "Not attached”

    b) Select "Storage" on the left side panel, in the "Storage Devices" area, click the icon that looks like a CD and is labeled "Empty", then in the "Attributes" area, click the icon that looks like a CD/DVD, select "Choose a virtual CD/DVD disk file", navigate to where the Windows 10 ISO is located and select Open

    c) Select "Display" on the left side panel. In the change the "Scale Factor:" box dependent on host video resolution, then select “OK”

        (1) FHD 1920 x 1080, leave display set to 100%

        (2) QHD 2560 x 1440, set display to 200%,

        (3) UHD 3840 x 2160, set display to 300%

10. In the "Oracle VM VirtualBox Manager" window, verify the Windows settings

11. Select the "Start" button to load the Win10-Ent-1 VM

12. When the Windows screen is presented, select “Next”, then select “Install now”. Follow the install prompts to configure and install Windows 10

    a) Tic the box for “I accept the license terms, select “Next”

b) At “Which type of installation do you want?”, select the “Custom: Install Windows only (advanced)” section

c) At “Where do you want to install Windows”, select “Next”

d) Continue to follow prompts for installation configuration

e) At “Let’s connect you to a network”, select “I don’t have internet” in the lower-left corner

f) At “There’s more to discover when you connect to the internet”, select “Continue with limited setup” in the lower-left corner

g) Follow prompts to create user, password, and security questions

h) At “Choose privacy settings for you device”, select “No” for all options, select “Accept”

i) At “Let Cortana help you get things done”, select “Not now”

13. Once Windows has rebooted and completes the installation process, a few more changes are required

a) Select the >Start >Settings >System >About >Rename this PC, set “Current PC name” to “Win10-Ent-1, select “Next”, then select “Restart now”, then log into the Win10-Ent-1 VM

b) Select >Start, then start typing “advanced” and select “Windows Defender Firewall with Advanced Security”

c) Select “Inbound Rules” in the left window

d) Scroll down to the rules starting with “File and Printer Sharing (Echo Request – ICMPv4-In)” (there are 2 rules for IPv4 and 2 rules for IPv6)

e) Select all 4 rules and select “Enable Rule” in the right-side panel

f) Right-click on each rule that has “Private” in the “Profile” column and select “Properties” (there is 1 rule each for IPv4 and IPv6)

(1) Select the “Scope” tab, then select the “Any IP address” button in the “Remote IP address” section, then select “OK”. Close this window and the admin tools window.

g) Close the “Windows Defender Firewall with Advanced Security” window

14. Right-click the Windows Start button, select “Shut down or sign out”, select “Shut down”

15. Select the “Settings” icon for the Windows VM

a) Select "Storage" on the left side panel, in the "Storage Devices" area, click the icon that looks like a CD and is labeled "19044.1288.211006-0501…", then in the "Attributes" area, click the icon that looks like a CD/DVD, select "Remove Disck from Virtual Drive”", select OK

16. Clone the Win10-Ent 1 VM

a) In the "Oracle VM VirtualBox Manager" window, right-click the Win10-Ent-1 VM and select “Clone”

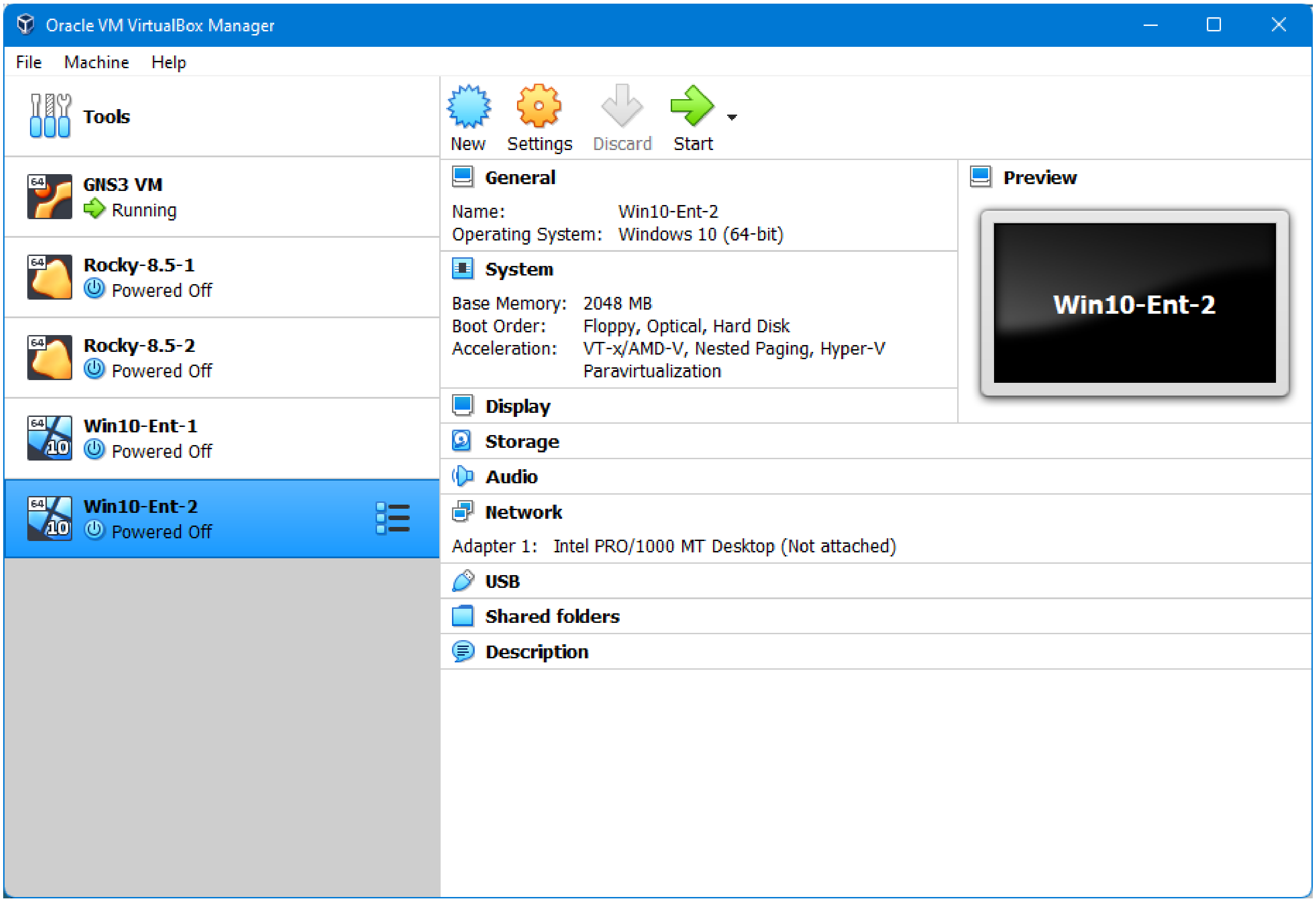
b) Set Name: to Win10-Ent-2, select “Next”

c) Verify the “Full clone” button is selected, select “Clone”

17. Start the Win10-Ent-2 VM, login

a) Select the >Start >Settings >System >About >Rename this PC, set “Current PC name” to “Win10-Ent-2, select “Next”, then select “Restart now”, then log into the Win10-Ent-2 VM

18. Right-click the Windows Start button, select “Shut down or sign out”, select “Shut down”



GNS3 VM
Running

Rocky-8.5-1
Powered Off

Rocky-8.5-2
Powered Off

Win10-Ent-1
Powered Off

Win10-Ent-2
Powered Off

Name: Win10-Ent-2
Operating System: Windows 10 (64-bit)

Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, Hyper-V Paravirtualization

Adapter 1: Intel PRO/1000 MT Desktop (Not attached)

XIII. Configuring the Wireshark-BYOL project, add the Windows 10 VMs

1. Add the windows 10 VMs to the project: in the Wireshark-BYOL – GNS3 window, select >Edit >Preferences >VirtualBox VMs

   a) Select New, in "Server" window select "Next", in VirtualBox Virtual Machine select Win10-Ent-1 then select "Finish"

   b) Select New, in "Server" window select "Next", in VirtualBox Virtual Machine select Win10-Ent-2 then select "Finish", then select "OK"

2. In the Wireshark-BYOL – GNS3 window, select the "Browse End Devices" icon in the left-side navigation

3. Click and drag the Win10-Ent-1 icon to the mid-lower-left of the projects main screen, below the left corner of the Switch1 icon

4. Click and drag the Win10-Ent-2 icon to the mid-lower-right of the projects main screen, below the right corner of the Switch2 icon

   a) click the "Browse End Devices" icon again to close the window

5. Align icons as needed

6. Connect the Windows VMs to the switch

   a) click the "Add a link" icon in the left-side navigation

   b) select the Win10-Ent-1-1 icon, select eth0

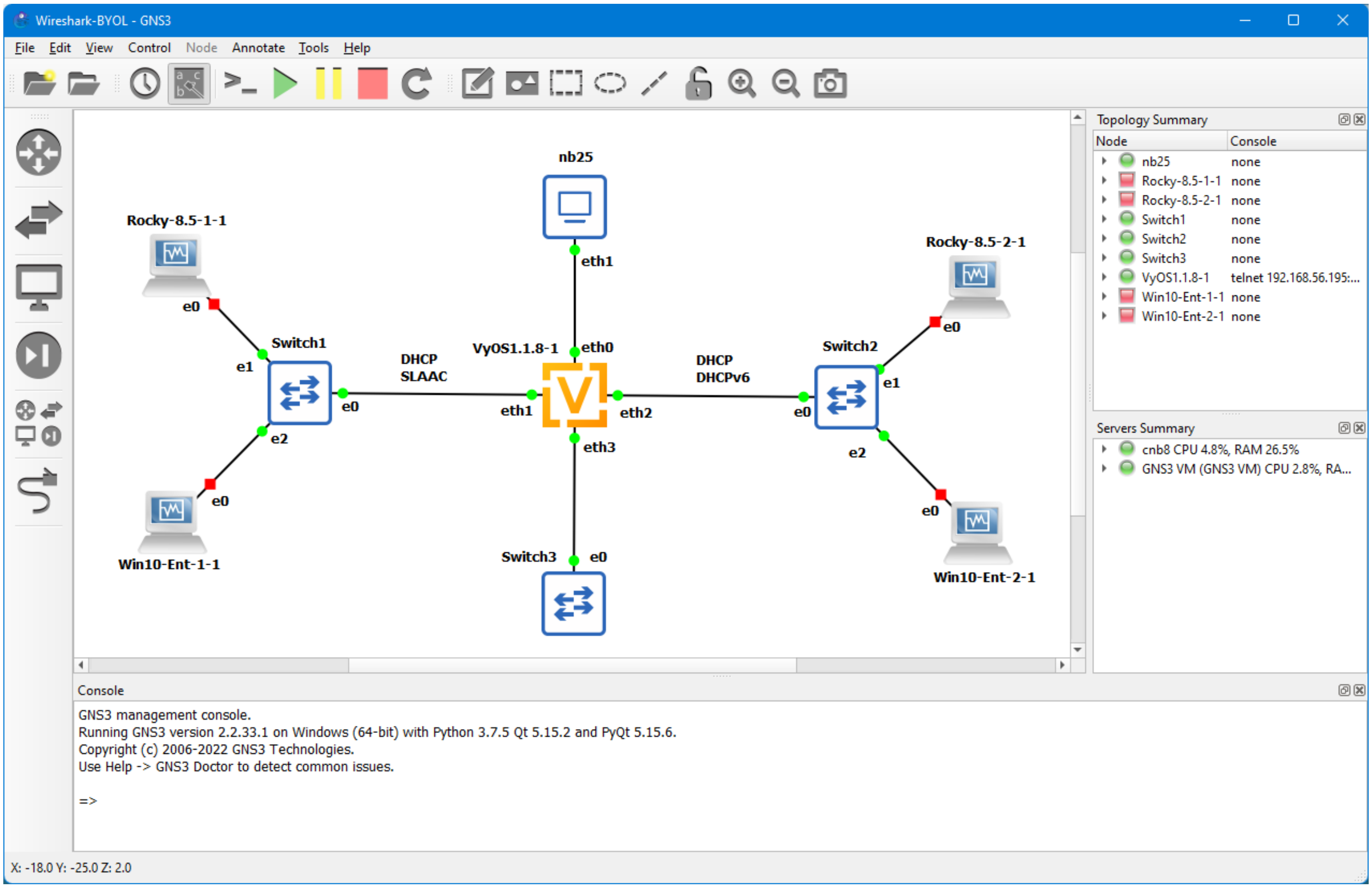
   c) select the Switch1 icon, select eth2

   d) select the Win10-Ent-2-1 icon, select eth0

   e) select the Switch2 icon, select eth2

   f) click the "Add a link" icon again to exit adding links

7. Adjust labels/icons as needed for viewing clarity



Topology Summary

Node	Console
nb25	none
Rocky-8.5-1-1	none
Rocky-8.5-2-1	none
Switch1	none
Switch2	none
Switch3	none
VyOS1.1.8-1	telnet 192.168.56.195:...
Win10-Ent-1-1	none
Win10-Ent-2-1	none

Servers Summary

- cnb8 CPU 4.8%, RAM 26.5%
- GNS3 VM (GNS3 VM) CPU 2.8%, RA...

Console

```
GNS3 management console.
Running GNS3 version 2.2.33.1 on Windows (64-bit) with Python 3.7.5 Qt 5.15.2 and PyQt 5.15.6.
Copyright (c) 2006-2022 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=>
```

X: -18.0 Y: -25.0 Z: 2.0

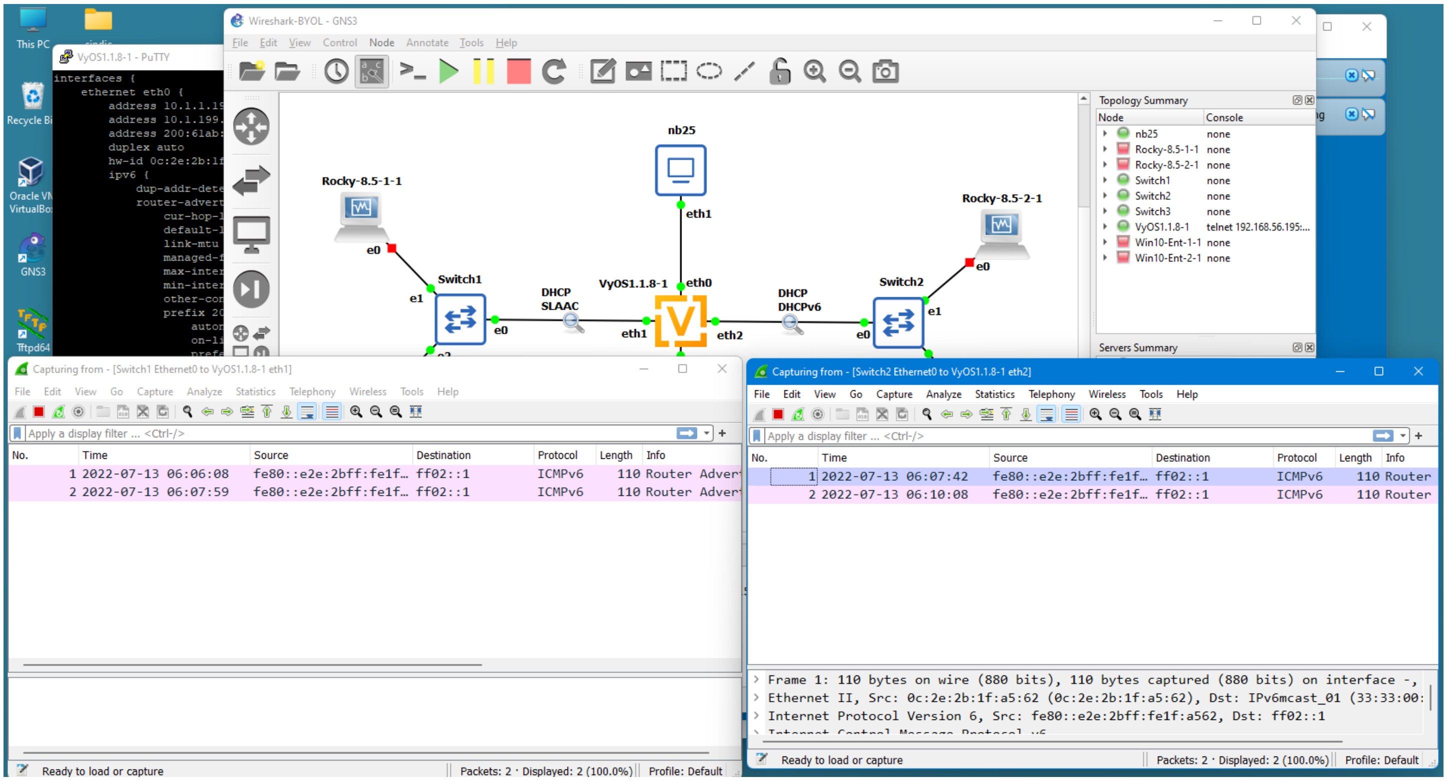
XIV. Start Captures and VMs

1. Start 2 capture sessions:

a) in the Wireshark-BYOL – GNS3 window, right-click on the link between Swtich1 and VyOS1.1.8-1, select "Start capture", then select "OK", this will launch a Wireshark capture. You will observe a small "magnifying icon on the link. Adjust the Wireshark application window to a smaller size in order to see additional windows.

b) in the Wireshark-BYOL – GNS3 window, right-click on the link between Swtich2 and VyOS1.1.8-1, select "Start capture", then select "OK", this will launch a Wireshark capture. You will observe a small "magnifying icon on the link. Adjust the Wireshark application window to a smaller size in order to see additional windows.

c) You will observe traffic is occurring, at least you should see ICMPv6 Router Advertisements on both network segments


This PC
Recycle Bi
Oracle VI
VirtualBo
GNS3
Tftpd64
VyOS1.1.8-1 - PuTTY
Wireshark-BYOL - GNS3
File Edit View Control Node Annotate Tools Help
nb25
eth1
Rocky-8.5-1-1
Rocky-8.5-2-1
e0
e1
Switch1
DHCP
SLAAC
VyOS1.1.8-1
eth0
e0
eth1
eth2
DHCP
DHCPv6
Switch2
e0
e1
e0
Topology Summary
Servers Summary
Capturing from - [Switch1 Ethernet0 to VyOS1.1.8-1 eth1]
Capturing from - [Switch2 Ethernet0 to VyOS1.1.8-1 eth2]
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
interfaces {
    ethernet eth0 {
        address 10.1.1.19
        address 10.1.199.
        address 200:61ab:
        duplex auto
        hw-id 0c:2e:2b:1f
        ipv6 {
            dup-addr-dete
            router-advert
                cur-hop-l
                default-l
                link-mtu
                managed-f
                max-inter
                min-inter
                other-con
                prefix 20
                    auton
                    on-li
```

Node	Console
nb25	none
Rocky-8.5-1-1	none
Rocky-8.5-2-1	none
Switch1	none
Switch2	none
Switch3	none
VyOS1.1.8-1	telnet 192.168.56.195:...
Win10-Ent-1-1	none
Win10-Ent-2-1	none

```
No.    Time                 Source               Destination  Protocol  Length Info
     1 2022-07-13 06:06:08  fe80::e2e:2bff:fe1f… ff02::1      ICMPv6       110 Router Adver
     2 2022-07-13 06:07:59  fe80::e2e:2bff:fe1f… ff02::1      ICMPv6       110 Router Adver
```

Ready to load or capture | Packets: 2 · Displayed: 2 (100.0%) | Profile: Default

```
No.    Time                 Source               Destination  Protocol  Length Info
     1 2022-07-13 06:07:42  fe80::e2e:2bff:fe1f… ff02::1      ICMPv6       110 Router
     2 2022-07-13 06:10:08  fe80::e2e:2bff:fe1f… ff02::1      ICMPv6       110 Router
```

```
> Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface -,
> Ethernet II, Src: 0c:2e:2b:1f:a5:62 (0c:2e:2b:1f:a5:62), Dst: IPv6mcast_01 (33:33:00:
> Internet Protocol Version 6, Src: fe80::e2e:2bff:fe1f:a562, Dst: ff02::1
```

Ready to load or capture | Packets: 2 · Displayed: 2 (100.0%) | Profile: Default

2. Start Rocky-8.5-1 VM

a) In the Wireshark-BYOL – GNS3 window, right-click the Rocky-8.5-1-1 and select "Start". GNS3 will communicate to VirtualBox and start the VM, a new VirtualBox session window will also popup for the Rocky Linux VM access

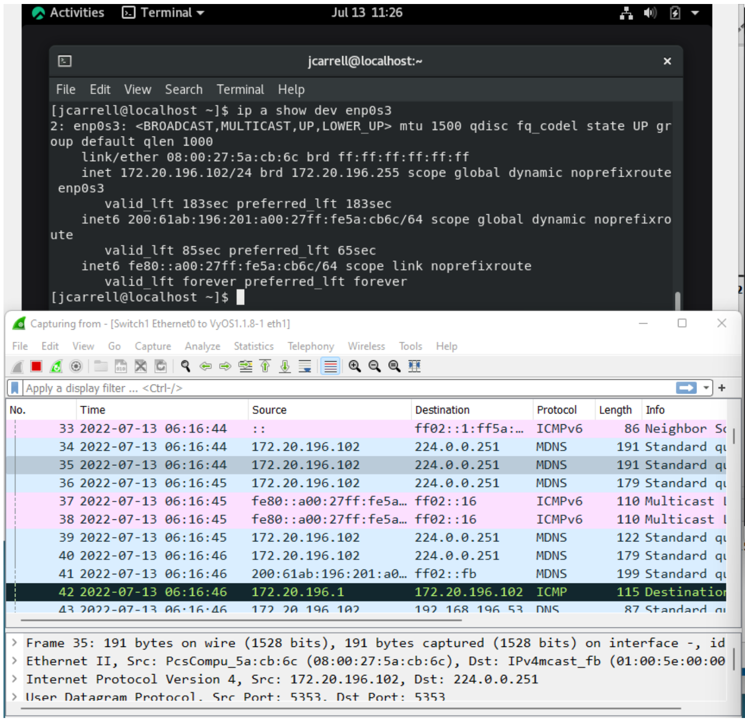
b) In the Rocky-8.5-1 [Running] – Oracle VM Virtual box window, login to the Rocky Linux VM

c) In the upper-right corner of the Rocky VM, select the "down arrow" button, select the right-facing arrow at Wired Off, select "connect"

d) Observe more traffic in the Wireshark capture window

e) Open a terminal session, enter "ip -a show dev enp0s3", observe the IPv4 and IPv6 addresses

3. Repeat process for Rocky-8.5.2

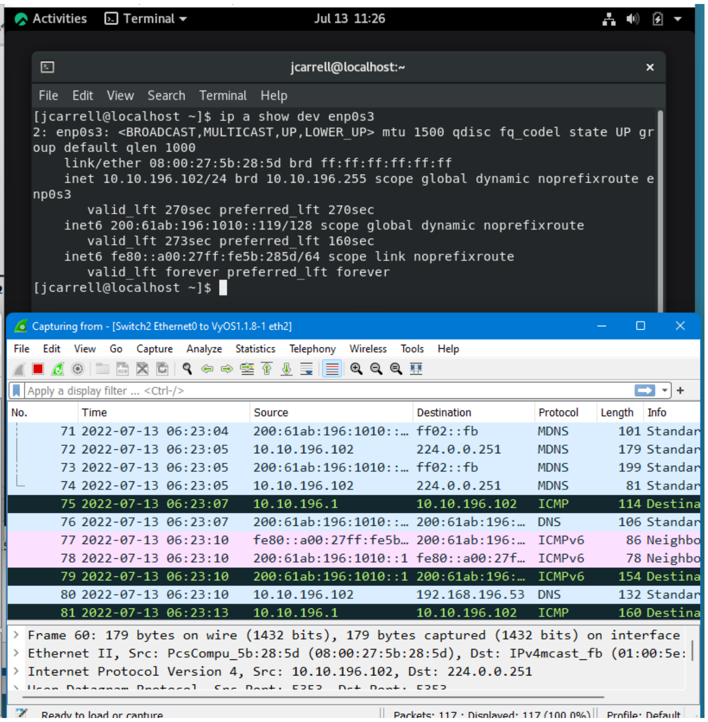


```
[jcarrell@localhost ~]$ ip a show dev enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:5a:cb:6c brd ff:ff:ff:ff:ff:ff
    inet 172.20.196.102/24 brd 172.20.196.255 scope global dynamic noprefixroute
 enp0s3
       valid_lft 183sec preferred_lft 183sec
    inet6 200:61ab:196:201:a00:27ff:fe5a:cb6c/64 scope global dynamic noprefixro
ute
       valid_lft 85sec preferred_lft 65sec
    inet6 fe80::a00:27ff:fe5a:cb6c/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[jcarrell@localhost ~]$
```

Capturing from - [Switch1 Ethernet0 to VyOS1.1.8-1 eth1]
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
33	2022-07-13 06:16:44	::	ff02::1:ff5a:…	ICMPv6	86	Neighbor Sc
34	2022-07-13 06:16:44	172.20.196.102	224.0.0.251	MDNS	191	Standard qu
35	2022-07-13 06:16:44	172.20.196.102	224.0.0.251	MDNS	191	Standard qu
36	2022-07-13 06:16:45	172.20.196.102	224.0.0.251	MDNS	179	Standard qu
37	2022-07-13 06:16:45	fe80::a00:27ff:fe5a…	ff02::16	ICMPv6	110	Multicast L
38	2022-07-13 06:16:45	fe80::a00:27ff:fe5a…	ff02::16	ICMPv6	110	Multicast L
39	2022-07-13 06:16:45	172.20.196.102	224.0.0.251	MDNS	122	Standard qu
40	2022-07-13 06:16:46	172.20.196.102	224.0.0.251	MDNS	179	Standard qu
41	2022-07-13 06:16:46	200:61ab:196:201:a0…	ff02::fb	MDNS	199	Standard qu
42	2022-07-13 06:16:46	172.20.196.1	172.20.196.102	ICMP	115	Destination
43	2022-07-13 06:16:46	172.20.196.102	192.168.196.53	DNS	87	Standard qu

```
> Frame 35: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits) on interface -, id
> Ethernet II, Src: PcsCompu_5a:cb:6c (08:00:27:5a:cb:6c), Dst: IPv4mcast_fb (01:00:5e:00:00
> Internet Protocol Version 4, Src: 172.20.196.102, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
```



```
[jcarrell@localhost ~]$ ip a show dev enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:5b:28:5d brd ff:ff:ff:ff:ff:ff
    inet 10.10.196.102/24 brd 10.10.196.255 scope global dynamic noprefixroute e
np0s3
       valid_lft 270sec preferred_lft 270sec
    inet6 200:61ab:196:1010::119/128 scope global dynamic noprefixroute
       valid_lft 273sec preferred_lft 160sec
    inet6 fe80::a00:27ff:fe5b:285d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[jcarrell@localhost ~]$
```

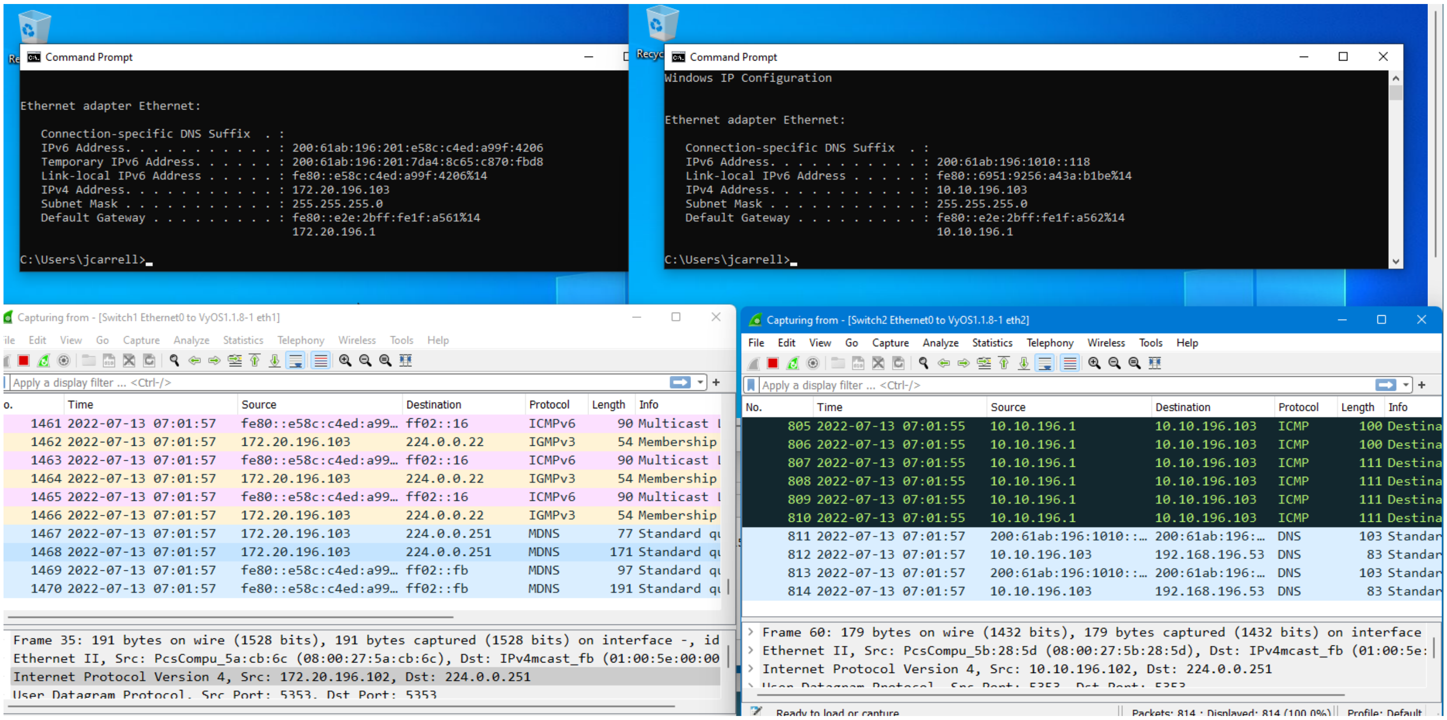
Capturing from - [Switch2 Ethernet0 to VyOS1.1.8-1 eth2]
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
71	2022-07-13 06:23:04	200:61ab:196:1010::…	ff02::fb	MDNS	101	Standar
72	2022-07-13 06:23:05	10.10.196.102	224.0.0.251	MDNS	179	Standar
73	2022-07-13 06:23:05	200:61ab:196:1010::…	ff02::fb	MDNS	199	Standar
74	2022-07-13 06:23:05	10.10.196.102	224.0.0.251	MDNS	81	Standar
75	2022-07-13 06:23:07	10.10.196.1	10.10.196.102	ICMP	114	Destina
76	2022-07-13 06:23:07	200:61ab:196:1010::…	200:61ab:196:…	DNS	106	Standar
77	2022-07-13 06:23:10	fe80::a00:27ff:fe5b…	200:61ab:196:…	ICMPv6	86	Neighbo
78	2022-07-13 06:23:10	200:61ab:196:1010::1	fe80::a00:27f…	ICMPv6	78	Neighbo
79	2022-07-13 06:23:10	200:61ab:196:1010::1	200:61ab:196:…	ICMPv6	154	Destina
80	2022-07-13 06:23:10	10.10.196.102	192.168.196.53	DNS	132	Standar
81	2022-07-13 06:23:13	10.10.196.1	10.10.196.102	ICMP	160	Destina

```
> Frame 60: 179 bytes on wire (1432 bits), 179 bytes captured (1432 bits) on interface
> Ethernet II, Src: PcsCompu_5b:28:5d (08:00:27:5b:28:5d), Dst: IPv4mcast_fb (01:00:5e:
> Internet Protocol Version 4, Src: 10.10.196.102, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
```

Ready to load or capture | Packets: 117 · Displayed: 117 (100.0%) | Profile: Default

4. Can repeat similar process for Windows VMs



Command Prompt

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 200:61ab:196:201:e58c:c4ed:a99f:4206
   Temporary IPv6 Address. . . . . . : 200:61ab:196:201:7da4:8c65:c870:fbd8
   Link-local IPv6 Address . . . . . : fe80::e58c:c4ed:a99f:4206%14
   IPv4 Address. . . . . . . . . . . : 172.20.196.103
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::e2e:2bff:fe1f:a561%14
                                       172.20.196.1

C:\Users\jcarrell>
```

Command Prompt

```
Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 200:61ab:196:1010::118
   Link-local IPv6 Address . . . . . : fe80::6951:9256:a43a:b1be%14
   IPv4 Address. . . . . . . . . . . : 10.10.196.103
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::e2e:2bff:fe1f:a562%14
                                       10.10.196.1

C:\Users\jcarrell>
```

Capturing from - [Switch1 Ethernet0 to VyOS1.1.8-1 eth1]

ile Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
o.     Time                 Source                  Destination   Protocol  Length Info
  1461 2022-07-13 07:01:57  fe80::e58c:c4ed:a99… ff02::16      ICMPv6       90 Multicast L
  1462 2022-07-13 07:01:57  172.20.196.103       224.0.0.22    IGMPv3       54 Membership
  1463 2022-07-13 07:01:57  fe80::e58c:c4ed:a99… ff02::16      ICMPv6       90 Multicast L
  1464 2022-07-13 07:01:57  172.20.196.103       224.0.0.22    IGMPv3       54 Membership
  1465 2022-07-13 07:01:57  fe80::e58c:c4ed:a99… ff02::16      ICMPv6       90 Multicast L
  1466 2022-07-13 07:01:57  172.20.196.103       224.0.0.22    IGMPv3       54 Membership
  1467 2022-07-13 07:01:57  172.20.196.103       224.0.0.251   MDNS         77 Standard qu
  1468 2022-07-13 07:01:57  172.20.196.103       224.0.0.251   MDNS        171 Standard qu
  1469 2022-07-13 07:01:57  fe80::e58c:c4ed:a99… ff02::fb      MDNS         97 Standard qu
  1470 2022-07-13 07:01:57  fe80::e58c:c4ed:a99… ff02::fb      MDNS        191 Standard qu

Frame 35: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits) on interface -, id
Ethernet II, Src: PcsCompu_5a:cb:6c (08:00:27:5a:cb:6c), Dst: IPv4mcast_fb (01:00:5e:00:00
Internet Protocol Version 4, Src: 172.20.196.102, Dst: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
```

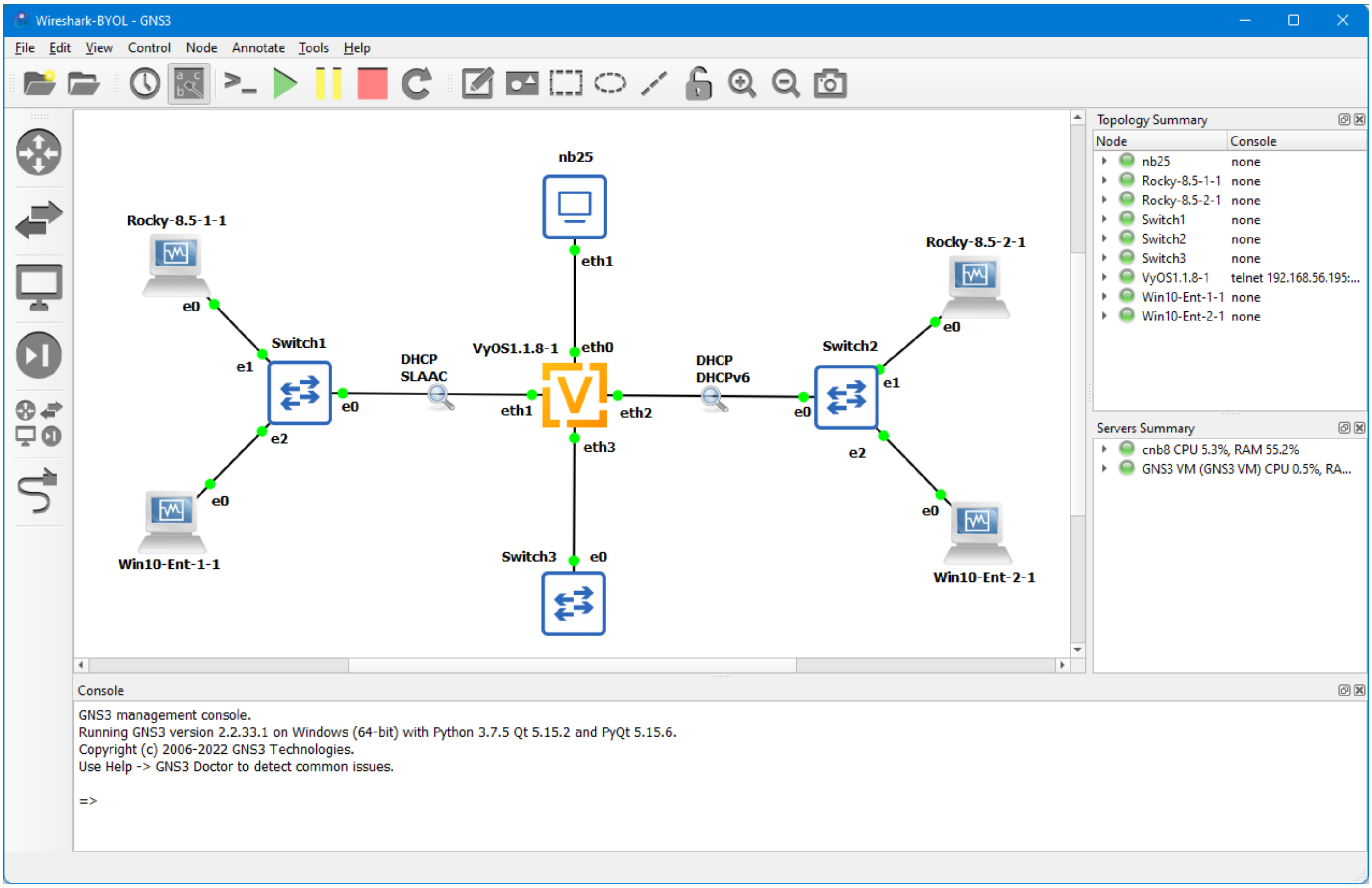
Capturing from - [Switch2 Ethernet0 to VyOS1.1.8-1 eth2]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.    Time                 Source                 Destination       Protocol  Length Info
   805 2022-07-13 07:01:55  10.10.196.1            10.10.196.103     ICMP        100 Destina
   806 2022-07-13 07:01:55  10.10.196.1            10.10.196.103     ICMP        100 Destina
   807 2022-07-13 07:01:55  10.10.196.1            10.10.196.103     ICMP        111 Destina
   808 2022-07-13 07:01:55  10.10.196.1            10.10.196.103     ICMP        111 Destina
   809 2022-07-13 07:01:55  10.10.196.1            10.10.196.103     ICMP        111 Destina
   810 2022-07-13 07:01:55  10.10.196.1            10.10.196.103     ICMP        111 Destina
   811 2022-07-13 07:01:57  200:61ab:196:1010::…   200:61ab:196:…    DNS         103 Standar
   812 2022-07-13 07:01:57  10.10.196.103          192.168.196.53    DNS          83 Standar
   813 2022-07-13 07:01:57  200:61ab:196:1010::…   200:61ab:196:…    DNS         103 Standar
   814 2022-07-13 07:01:57  10.10.196.103          192.168.196.53    DNS          83 Standar

> Frame 60: 179 bytes on wire (1432 bits), 179 bytes captured (1432 bits) on interface
> Ethernet II, Src: PcsCompu_5b:28:5d (08:00:27:5b:28:5d), Dst: IPv4mcast_fb (01:00:5e:
> Internet Protocol Version 4, Src: 10.10.196.102, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353

Ready to load or capture     Packets: 814 · Displayed: 814 (100.0%)     Profile: Default
```



Wireshark-BYOL - GNS3

Topology Summary

Node	Console
nb25	none
Rocky-8.5-1-1	none
Rocky-8.5-2-1	none
Switch1	none
Switch2	none
Switch3	none
VyOS1.1.8-1	telnet 192.168.56.195:...
Win10-Ent-1-1	none
Win10-Ent-2-1	none

Servers Summary

- cnb8 CPU 5.3%, RAM 55.2%
- GNS3 VM (GNS3 VM) CPU 0.5%, RA...

Console

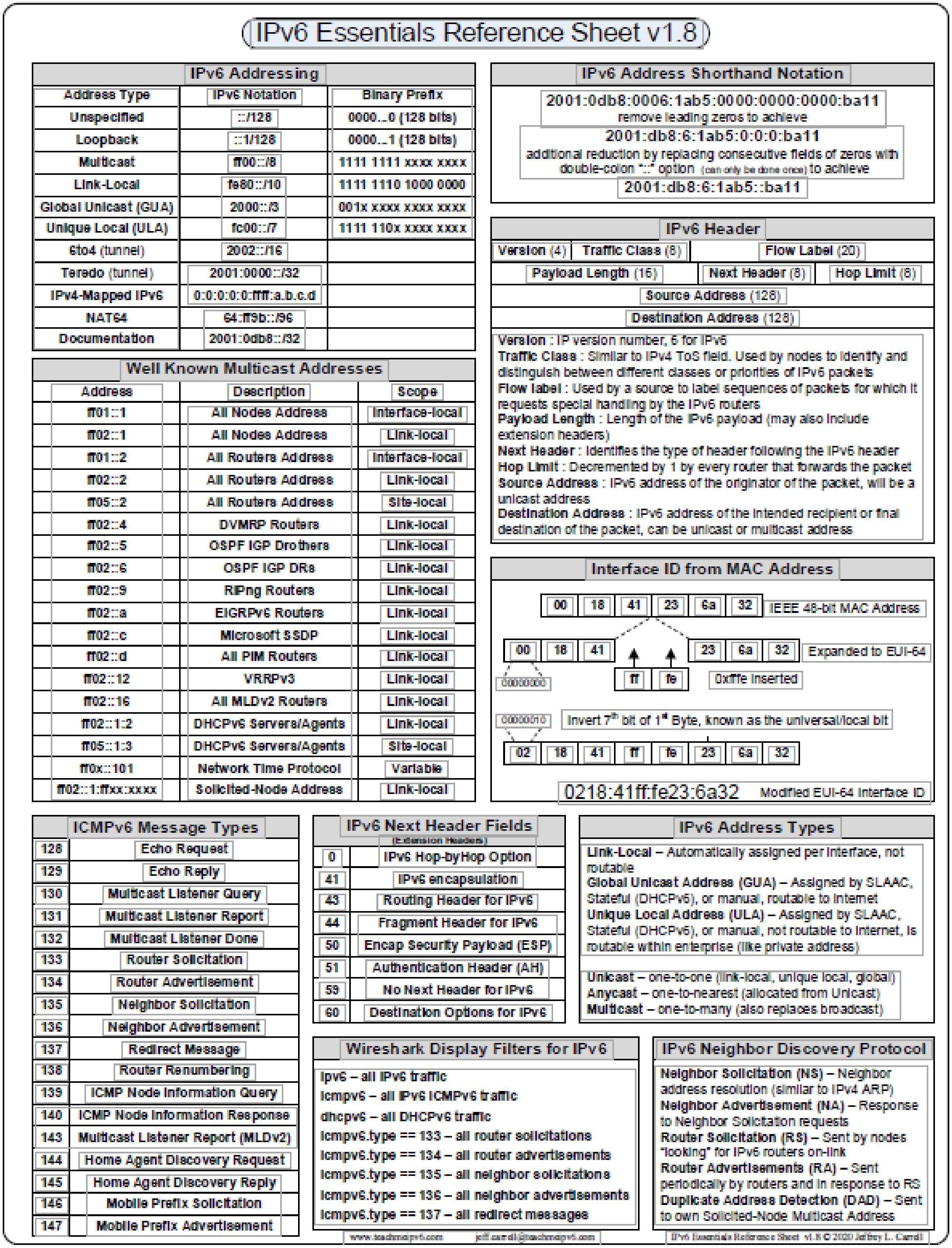
```
GNS3 management console.
Running GNS3 version 2.2.33.1 on Windows (64-bit) with Python 3.7.5 Qt 5.15.2 and PyQt 5.15.6.
Copyright (c) 2006-2022 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=>
```

Congratulations, you are on the way for your Wireshark journey!

XV. Appendix

A. IPv6 Essentials Reference Sheet



IPv6 Essentials Reference Sheet v1.8

IPv6 Addressing

Address Type	IPv6 Notation	Binary Prefix
Unspecified	::/128	0000...0 (128 bits)
Loopback	::1/128	0000...1 (128 bits)
Multicast	ff00::/8	1111 1111 xxxx xxxx
Link-Local	fe80::/10	1111 1110 1000 0000
Global Unicast (GUA)	2000::/3	001x xxxx xxxx xxxx
Unique Local (ULA)	fc00::/7	1111 110x xxxx xxxx
6to4 (tunnel)	2002::/16	
Teredo (tunnel)	2001:0000::/32	
IPv4-Mapped IPv6	0:0:0:0:0:ffff:a.b.c.d	
NAT64	64:ff9b::/96	
Documentation	2001:0db8::/32	

Well Known Multicast Addresses

Address	Description	Scope
ff01::1	All Nodes Address	Interface-local
ff02::1	All Nodes Address	Link-local
ff01::2	All Routers Address	Interface-local
ff02::2	All Routers Address	Link-local
ff05::2	All Routers Address	Site-local
ff02::4	DVMRP Routers	Link-local
ff02::5	OSPF IGP Drothers	Link-local
ff02::6	OSPF IGP DRs	Link-local
ff02::9	RIPng Routers	Link-local
ff02::a	EIGRPv6 Routers	Link-local
ff02::c	Microsoft SSDP	Link-local
ff02::d	All PIM Routers	Link-local
ff02::12	VRRPv3	Link-local
ff02::16	All MLDv2 Routers	Link-local
ff02::1:2	DHCPv6 Servers/Agents	Link-local
ff05::1:3	DHCPv6 Servers/Agents	Site-local
ff0x::101	Network Time Protocol	Variable
ff02::1:ffxx:xxxx	Solicited-Node Address	Link-local

IPv6 Address Shorthand Notation

2001:0db8:0006:1ab5:0000:0000:0000:ba11

remove leading zeros to achieve

2001:db8:6:1ab5:0:0:0:ba11

additional reduction by replacing consecutive fields of zeros with double-colon "::" option (can only be done once) to achieve

2001:db8:6:1ab5::ba11

IPv6 Header

Version (4)	Traffic Class (8)	Flow Label (20)	
Payload Length (16)		Next Header (8)	Hop Limit (8)
Source Address (128)			
Destination Address (128)			

Version : IP version number, 6 for IPv6
Traffic Class : Similar to IPv4 ToS field. Used by nodes to identify and distinguish between different classes or priorities of IPv6 packets
Flow label : Used by a source to label sequences of packets for which it requests special handling by the IPv6 routers
Payload Length : Length of the IPv6 payload (may also include extension headers)
Next Header : Identifies the type of header following the IPv6 header
Hop Limit : Decremented by 1 by every router that forwards the packet
Source Address : IPv6 address of the originator of the packet, will be a unicast address
Destination Address : IPv6 address of the intended recipient or final destination of the packet, can be unicast or multicast address

Interface ID from MAC Address

00 | 18 | 41 | 23 | 6a | 32 — IEEE 48-bit MAC Address

00 | 18 | 41 | | | 23 | 6a | 32 — Expanded to EUI-64

ff | fe — 0xfffe Inserted

00000000

00000010 — Invert 7th bit of 1st Byte, known as the universal/local bit

02 | 18 | 41 | ff | fe | 23 | 6a | 32

0218:41ff:fe23:6a32 — Modified EUI-64 Interface ID

ICMPv6 Message Types

128	Echo Request
129	Echo Reply
130	Multicast Listener Query
131	Multicast Listener Report
132	Multicast Listener Done
133	Router Solicitation
134	Router Advertisement
135	Neighbor Solicitation
136	Neighbor Advertisement
137	Redirect Message
138	Router Renumbering
139	ICMP Node Information Query
140	ICMP Node Information Response
143	Multicast Listener Report (MLDv2)
144	Home Agent Discovery Request
145	Home Agent Discovery Reply
146	Mobile Prefix Solicitation
147	Mobile Prefix Advertisement

IPv6 Next Header Fields
(Extension Headers)

0	IPv6 Hop-byHop Option
41	IPv6 encapsulation
43	Routing Header for IPv6
44	Fragment Header for IPv6
50	Encap Security Payload (ESP)
51	Authentication Header (AH)
59	No Next Header for IPv6
60	Destination Options for IPv6

IPv6 Address Types

Link-Local – Automatically assigned per interface, not routable
Global Unicast Address (GUA) – Assigned by SLAAC, Stateful (DHCPv6), or manual, routable to Internet
Unique Local Address (ULA) – Assigned by SLAAC, Stateful (DHCPv6), or manual, not routable to Internet, is routable within enterprise (like private address)

Unicast – one-to-one (link-local, unique local, global)
Anycast – one-to-nearest (allocated from Unicast)
Multicast – one-to-many (also replaces broadcast)

Wireshark Display Filters for IPv6

ipv6 – all IPv6 traffic
icmpv6 – all IPv6 ICMPv6 traffic
dhcpv6 – all DHCPv6 traffic
icmpv6.type == 133 – all router solicitations
icmpv6.type == 134 – all router advertisements
icmpv6.type == 135 – all neighbor solicitations
icmpv6.type == 136 – all neighbor advertisements
icmpv6.type == 137 – all redirect messages

IPv6 Neighbor Discovery Protocol

Neighbor Solicitation (NS) – Neighbor address resolution (similar to IPv4 ARP)
Neighbor Advertisement (NA) – Response to Neighbor Solicitation requests
Router Solicitation (RS) – Sent by nodes "looking" for IPv6 routers on-link
Router Advertisements (RA) – Sent periodically by routers and in response to RS
Duplicate Address Detection (DAD) – Sent to own Solicited-Node Multicast Address

www.teachmeipv6.com jeff.carrell@teachmeipv6.com

IPv6 Essentials Reference Sheet v1.8 © 2020 Jeffrey L. Carrell