

Lab 2: Dynamic Networking with GNS3 and VirtualBox VMs

This lab builds from the previous lab 1 using manual IP addressing. There are times when this method is used. One practical scenario is when host systems or services require constant IP addressing for consistent reference such as on DNS, web, email servers, etc. Otherwise, clients that rely on those services may lose connectivity if inconsistent IP addresses are allowed.

However, relying only on this approach can yield to all sorts of challenges. One such problem is the IP address *management overhead* to keep track of which address is already used to avoid duplicate designation. Such a manual method is also prone to *misconfigurations* since it is done by hand and people may potentially mistype information. Last, but not least, is the fact that it is simply *not scalable* to do this for every device that needs to connect to the network particularly when those hosts do not require to keep a particular address.

The goal of this lab is to identify how dynamic IP addressing works. One must also know how to configure a Dynamic Host Configuration Protocol (DHCP) server to host a pool of assignable IP address range. You will configure the Endian VM's internal LAN to be on a specific private network and enable DHCP service to lease its available IP address pool to any requesting client on the network rather than relying on static assignments. This is done within GNS3 along with Wireshark to analyze captured DHCP packets that pass through the virtual link connections adjacent to the switch. The captured DHCP traffic allows each client to lease an IP address.

Prerequisites:

- Completion of Lab 1
- Wireshark
- Endian, Ubuntu, and Kali VMs

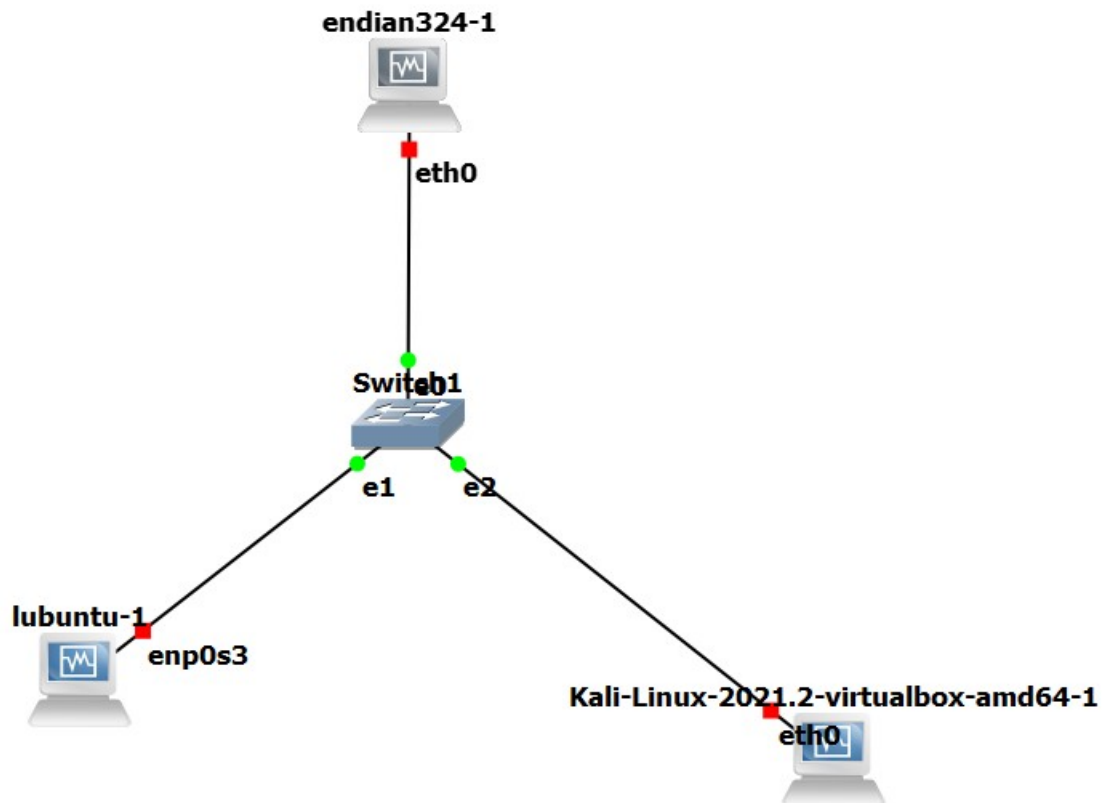
Note: Refer to "GNS3 with Virtualbox" to import and configure each VM.

To Do List:

- Provide answers to all of the yellow highlighted sections below to get full credit for this lab.
- Make a copy of this document and save it either locally or to your cloud storage such as Google/OneDrive drive, Dropbox, etc. **Edit your copy of the file to insert your answers. (3 pts)**
- **Lab report submission format: (2 pts)** `cpssc456-lab#-<insert-name-here>.{doc|pdf|docx|odt|rtf}`
 - E.g. using PDF, `cpssc456-lab2-hernan-manabat.pdf`

Let us build the GNS3 network topology!

1. Create a new GNS3 project. Add an Ethernet Switch, the Endian, Kali, and Ubuntu VMs to the topology from the device list. Connect all the VMs to the Ethernet Switch using the 'add a link' stencil. Make sure to connect the Endian VM's eth0 to the Ethernet Switch. Toggle the "Show/Hide Interface labels" to display network interfaces. **Take a screenshot of your network topology along with all the VMs (15 pts)**



2. **What are the given IP addresses of Ubuntu and Kali VMs? Use screenshots. (5 pts)**
Hint: Use the `ifconfig` or `ip` command
Ubuntu:

Due: Thursday, February 17, 2022 @ 11:59 PM

```

osboxes@osboxes:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
    group default qlen 1000
    link/ether 08:00:27:f2:24:bf brd ff:ff:ff:ff:ff:ff
    inet 10.0.1.4/24 brd 10.0.1.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::6bb3:f0db:f119:48d1/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

```

IP
addr

Kali:

```

(kali@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
    group default qlen 1000
    link/ether 08:00:27:0e:34:8d brd ff:ff:ff:ff:ff:ff
    inet 10.0.1.5/16 brd 10.0.255.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet 192.168.1.9/24 brd 192.168.1.255 scope global dynamic noprefixroute
        valid_lft 3558sec preferred_lft 3558sec
    inet6 fe80::a00:27ff:fe0e:348d/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

```

IP

3. What is the *default* network ID (subnet) used by the Endian VM? Use the CIDR notation. (5 pts)

```

Endian Demo [Running]
2021-02-19 11:02:20 SETPOLICYROUTING-I-Restart
Product: Community (64 bit)
Hostname: efw-561b914e2c

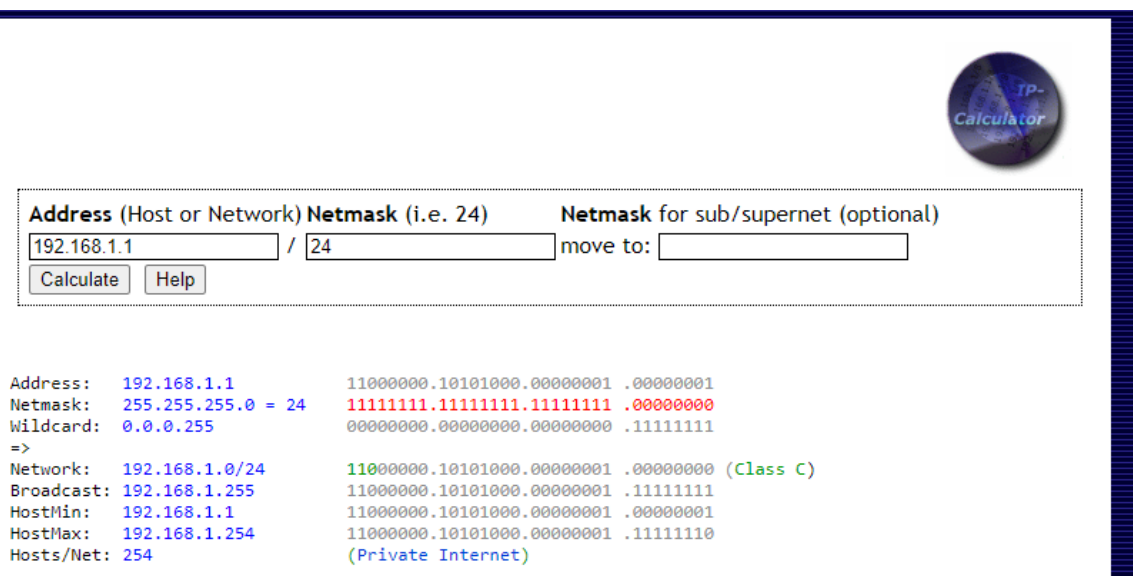
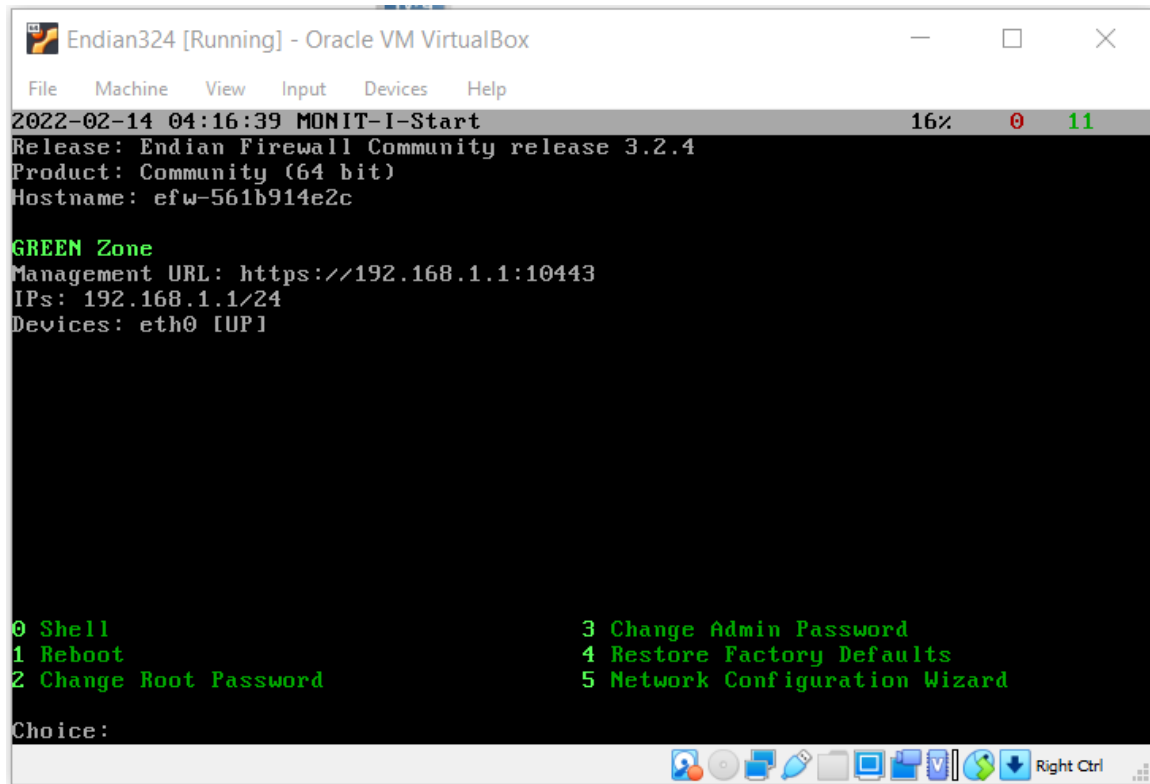
GREEN Zone
Management URL: https://192.168.1.1:10443
IPs: 192.168.1.1/24
Devices: eth0 [UP]

0 Shell
1 Reboot
2 Change Root Password
3 Change Admin Password
4 Restore Factory Defaults
5 Network Configuration Wizard

Choice: 5
Enter Root Password:

```

Due: Thursday, February 17, 2022 @ 11:59 PM



192.168.1.0/24

4. Configure the Endian VM to use the private subnet (172.20.22.0/24) on its eth0 (GREEN) interface:

To learn more about Endian Firewall's color-coded interfaces visit

http://docs.endian.com/archive/2.1/efw.system.network_configuration.html.

Due: Thursday, February 17, 2022 @ 11:59 PM

- a. Press 5 to enter the Network Configuration Wizard.
- b. Enter root's password: `endian` [enter]
- c. Hostname? `EFW-S22` [enter]
- d. Domain? `localdomain` [enter]
- e. RED interface type...? `DHCP` [enter]
- f. RED device <eth0/eth1>? `eth1` [enter]
Note: If you only see eth0, make sure your VirtualBox VM has two network interfaces configured in VirtualBox Manager and as a GNS3 VirtualBox VM template.
- g. Primary DNS? [enter]
- h. Secondary DNS? [enter]
- i. GREEN devices <eth0>? `eth0` [enter]
- j. GREEN IPs (IP/CIDR)? `10.20.22.254/24` [enter]
Note: This will be the IP address of your internal interface that will serve as your gateway.
- k. Enable DHCP server on GREEN: `on` [enter]
- l. ORANGE devices: [enter]
- m. ORANGE IPs (IP/CIDR): [enter]
- n. BLUE devices: [enter]
- o. BLUE IPs (IP/CIDR): [enter]
- p. Enable SSH access: `on` [enter]
- q. Allow access to ports 22, 80 and 10443 from any interface: `on` [enter]
- r. Is the above correct <yes/no>? `yes` [enter]
- s. Write configuration <yes/no>? `yes` [enter]

Take a screenshot of your Endian Firewall network configuration (10 pts)

Due: Thursday, February 17, 2022 @ 11:59 PM

```

2022-02-15 04:22:12 SETPOLICYROUTING-I-Restart
Domain: localdomain
RED interface type: DHCP
RED device: eth1
RED IPs (IP/CIDR):
RED gateway:
Primary DNS:
Secondary DNS:
GREEN devices: eth0
GREEN IPs (IP/CIDR): 10.20.22.254/24
Enable DHCP server on GREEN: on
ORANGE devices:
ORANGE IPs (IP/CIDR):
BLUE devices:
BLUE IPs (IP/CIDR):
Enable SSH access: on
Allow access to ports 22, 80 and 10443 from any interface: on

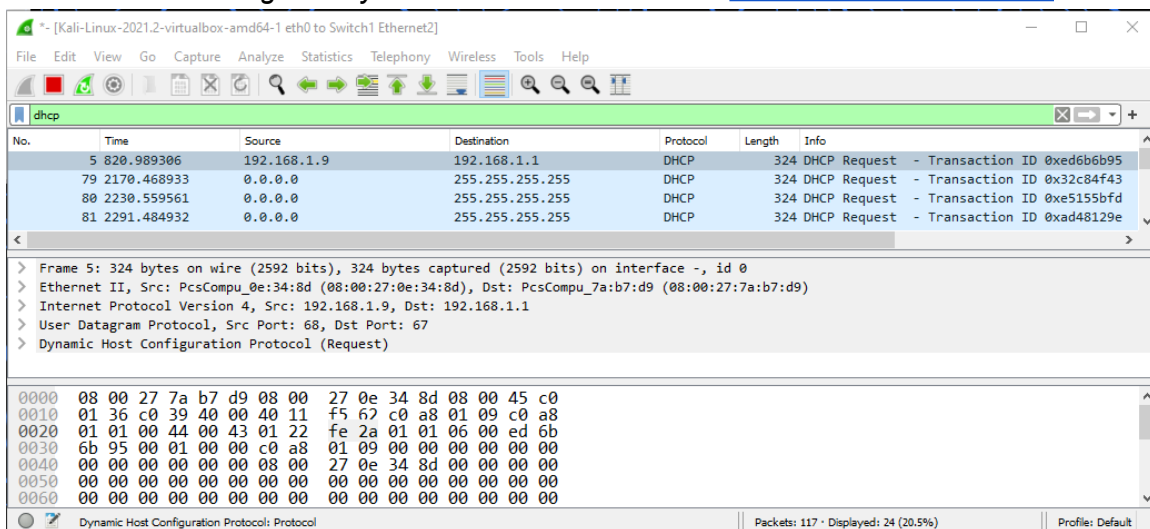
Is the above correct <yes/no>? yes
Write configuration <yes/no>? yes
Writing configuration...
Applying configuration...

Press ENTER_

```

- t. Press [enter] to finish the network configuration wizard.
5. Right-click on the link between kali in the Kali VM and the Ethernet Switch. Select **Start capture** to start a Wireshark window. Accept the default setting and hit the **OK** button when prompted. Type “dhcp” on the *display filter* search field to only show packets related to DHCP/BOOTP.

Use the following link if you need a refresher on the [introduction to Wireshark](#).



Due: Thursday, February 17, 2022 @ 11:59 PM

- Start all VMs and check the Wireshark window for DHCP network traffic. The DHCP DORA transactions will be visible if the Kali VM is successful in leasing an IP address from the DHCP server.

If not successful, verify that Kali is set to use an Automatic IP address and the eth0 interface is enabled. Then, open a command line on the Kali VM to lease an IPv4 address from the DHCP server (Endian VM).

```
$ sudo dhclient eth0
```

On the Wireshark window, you should see a similar sequence of 4 network packets listed below highlighted in blue as soon as the VM is fully started. If you are only seeing two DHCP packets (Request and ACK), reboot your VM and wait for the DHCP traffic to be captured. Take a similar screenshot of your Wireshark packet capture of the DHCP transactions (5 pts).

No.	Time	Source	Destination	Protocol	Length	Info
5	19.345341	172.20.21.2	172.20.21.254	DHCP	342	DHCP Release - Transaction ID 0x305fa6ea
6	29.220739	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xca0a86e1
8	30.223084	172.20.21.254	172.20.21.2	DHCP	342	DHCP Offer - Transaction ID 0xca0a86e1
9	30.223686	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xca0a86e1
10	30.225893	172.20.21.254	172.20.21.2	DHCP	342	DHCP ACK - Transaction ID 0xca0a86e1

mine:

No.	Time	Source	Destination	Protocol	Length	Info
29	10.021709	0.0.0.0	255.255.255.255	DHCP	330	DHCP Request - Transaction ID 0x7c57a1f0
36	12.021238	0.0.0.0	255.255.255.255	DHCP	330	DHCP Discover - Transaction ID 0x1887e2e9
40	14.464856	0.0.0.0	255.255.255.255	DHCP	330	DHCP Discover - Transaction ID 0x22028b00
44	18.691242	0.0.0.0	255.255.255.255	DHCP	330	DHCP Discover - Transaction ID 0x3848a54
46	27.675068	0.0.0.0	255.255.255.255	DHCP	330	DHCP Discover - Transaction ID 0xb6803eb
51	44.340813	0.0.0.0	255.255.255.255	DHCP	330	DHCP Discover - Transaction ID 0xc9400884
54	45.342656	10.20.22.254	10.20.22.1	DHCP	347	DHCP Offer - Transaction ID 0xc9400884
55	45.343606	0.0.0.0	255.255.255.255	DHCP	336	DHCP Request - Transaction ID 0xc9400884
56	45.358366	10.20.22.254	10.20.22.1	DHCP	347	DHCP ACK - Transaction ID 0xc9400884

> Frame 29: 330 bytes on wire (2640 bits), 330 bytes captured (2640 bits) on interface -, id 0

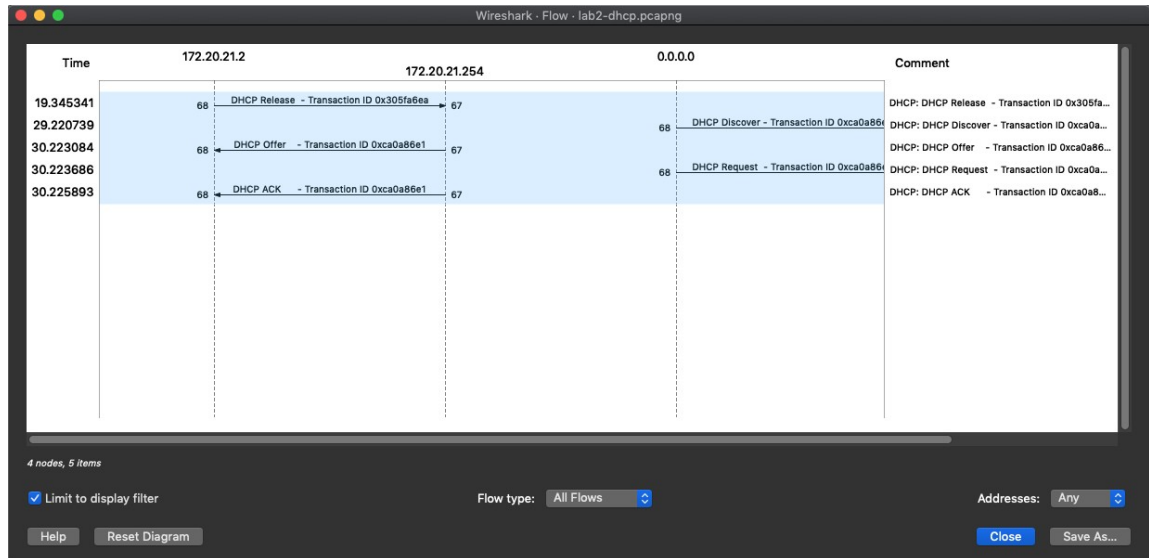
```

0000  ff ff ff ff ff ff 08 00 27 0e 34 8d 08 00 45 c0
0010  01 3c 00 00 00 40 00 40 11 38 f2 00 00 00 00 ff ff
0020  ff ff 00 44 00 43 01 28 24 91 01 01 06 00 7c 57
0030  a1 f0 00 01 00 00 00 00 00 00 00 00 00 00 00 00
0040  00 00 00 00 00 00 08 00 27 0e 34 8d 00 00 00 00
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  
```

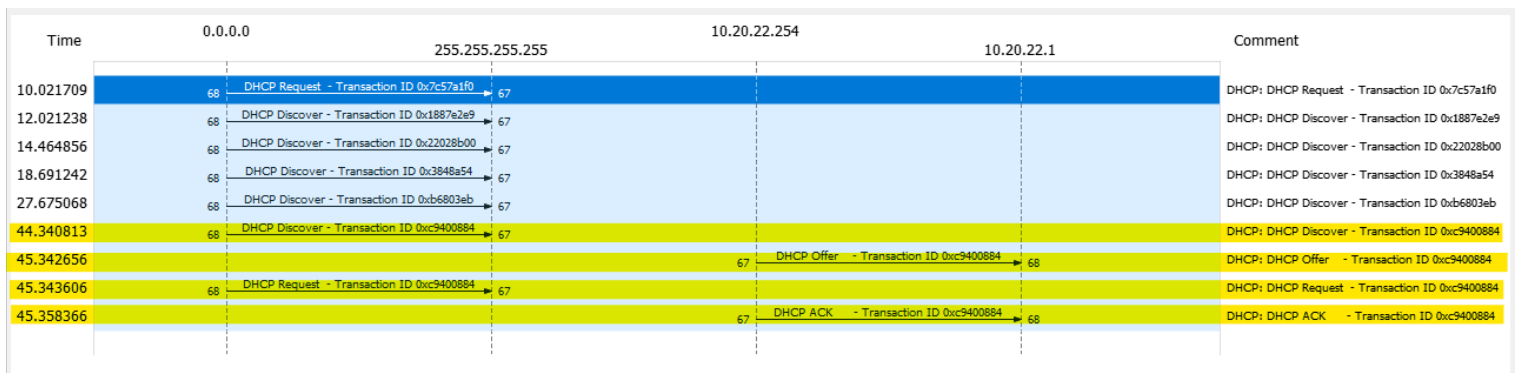
Dynamic Host Configuration Protocol: Protocol | Packets: 69 · Displayed: 9 (13.0%) | Profile: Default

- Stop the Wireshark packet capture and save it as “lab2-dhcp” on your computer. Go to the Statistics menu and select the flow graph to generate a timeline similar to the one below. Make sure to check the “Limit to Display Filter” to only show the DHCP transactions. Take a similar screenshot of your Wireshark packet capture of the DHCP transactions. Expand the window to show as much information as can be displayed of the transactions. (5 pts)

Due: Thursday, February 17, 2022 @ 11:59 PM



mine:



8. Give a detail explanation on how the client machine was able to get an IPv4 address from the DHCP server on the network starting from a successful DHCP Discover transaction using your captured flow graph. (15 pts) Hint: Explain DHCP (DORA) transactions based on the wireshark capture and timeline from #6 and #7.

Kali from 0.0.0.0 tries to discover a DHCP server.

Endian from 10.20.22.254 offers the IP address 10.20.22.1 to Kali.

Kali from 0.0.0.0 requests to have the IP address 10.20.22.1 that Endian is offering.

Endian acknowledges Kali's request and gives the IP address to Kali. Then the IP address of 10.20.22.1 is removed from the list of available IP addresses.

9. What is your given IPv4 address for the Kali and Ubuntu VMs? (5 pts)
Note: A loopback (127.0.0.1) address cannot be used outside your machine. Ignore any IPv6 address as well.

Due: Thursday, February 17, 2022 @ 11:59 PM

Lubuntu: 10.20.22.2 / 24

```
osboxes@osboxes:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
  ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
      valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
      valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
  group default qlen 1000
    link/ether 08:00:27:f2:24:bf brd ff:ff:ff:ff:ff:ff
    inet 10.20.22.2/24 brd 10.20.22.255 scope global dynamic noprefixroute en
  p0s3
    valid_lft 3576sec preferred_lft 3576sec
    inet6 fe80::6bb3:f0db:f119:48d1/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
```

IPV4

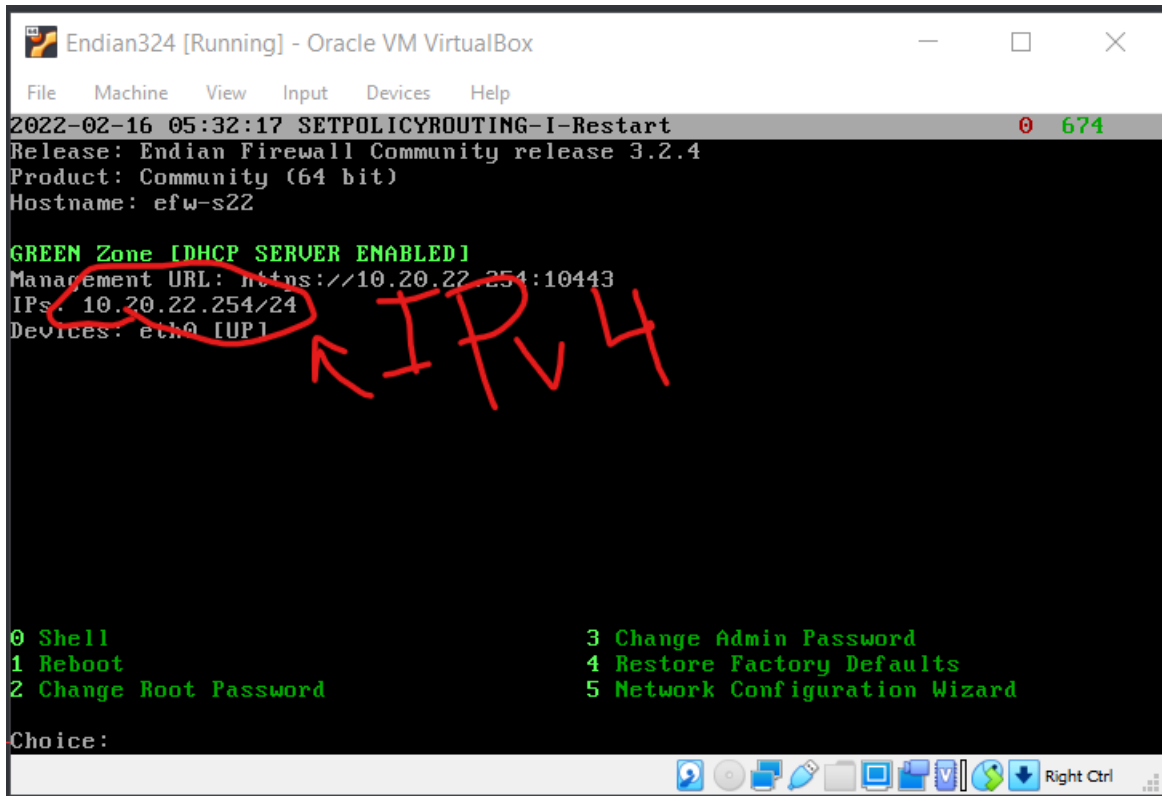
Kali: 10.20.22.1/24

```
(kali@kali)~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
  ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
      valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
      valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
  group default qlen 1000
    link/ether 08:00:27:0e:34:8d brd ff:ff:ff:ff:ff:ff
    inet 10.20.22.1/24 brd 10.20.22.255 scope global dynamic noprefixroute et
  h0
    valid_lft 3591sec preferred_lft 3591sec
    inet6 fe80::a00:27ff:fe0e:348d/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
```

IPV4

endian: 10.20.22.254/24

Due: Thursday, February 17, 2022 @ 11:59 PM



The screenshot shows a terminal window titled "Endian324 [Running] - Oracle VM VirtualBox". The terminal output includes the following text:

```
2022-02-16 05:32:17 SETPOLICYROUTING-I-Restart
Release: Endian Firewall Community release 3.2.4
Product: Community (64 bit)
Hostname: efw-s22

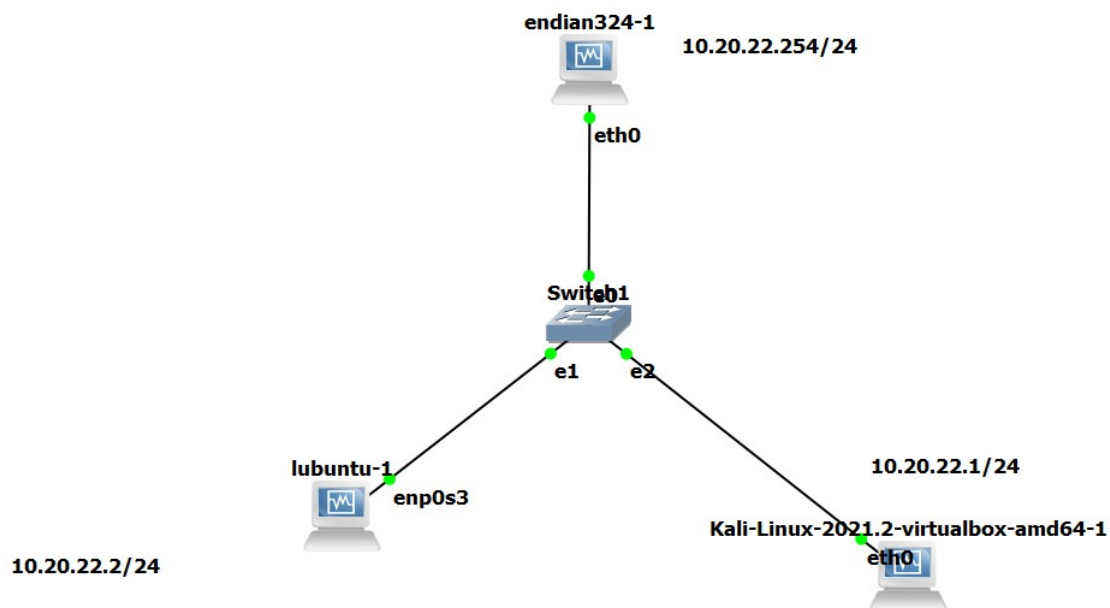
GREEN Zone [DHCP SERVER ENABLED]
Management URL: https://10.20.22.254:10443
IPs: 10.20.22.254/24
Devices: eth0 [UP]

0 Shell
1 Reboot
2 Change Root Password
3 Change Admin Password
4 Restore Factory Defaults
5 Network Configuration Wizard

Choice:
```

Handwritten red annotations are present: a circle around "10.20.22.254/24" and the text "IPV4" with an arrow pointing to the circled IP address.

gns3:



Due: Thursday, February 17, 2022 @ 11:59 PM

10. From the Kali VM, are you able to successfully ping both the Endian and Lubuntux86 VMs? (5 pts)

Lubuntu ping:

```
(kali㉿kali)-[~]  
$ ping 10.20.22.2  
PING 10.20.22.2 (10.20.22.2) 56(84) bytes of data.  
64 bytes from 10.20.22.2: icmp_seq=1 ttl=64 time=1.15 ms  
64 bytes from 10.20.22.2: icmp_seq=2 ttl=64 time=1.13 ms  
64 bytes from 10.20.22.2: icmp_seq=3 ttl=64 time=1.40 ms  
64 bytes from 10.20.22.2: icmp_seq=4 ttl=64 time=1.14 ms  
64 bytes from 10.20.22.2: icmp_seq=5 ttl=64 time=1.15 ms  
64 bytes from 10.20.22.2: icmp_seq=6 ttl=64 time=1.37 ms  
64 bytes from 10.20.22.2: icmp_seq=7 ttl=64 time=1.60 ms  
64 bytes from 10.20.22.2: icmp_seq=8 ttl=64 time=1.66 ms  
64 bytes from 10.20.22.2: icmp_seq=9 ttl=64 time=1.38 ms  
64 bytes from 10.20.22.2: icmp_seq=10 ttl=64 time=2.30 ms  
^C  
--- 10.20.22.2 ping statistics ---  
10 packets transmitted, 10 received, 0% packet loss, time 9295ms  
rtt min/avg/max/mdev = 1.128/1.426/2.298/0.342 ms
```

Endian ping:

```
(kali㉿kali)-[~]  
$ ping 10.20.22.254  
PING 10.20.22.254 (10.20.22.254) 56(84) bytes of data.  
64 bytes from 10.20.22.254: icmp_seq=1 ttl=64 time=1.50 ms  
64 bytes from 10.20.22.254: icmp_seq=2 ttl=64 time=1.34 ms  
64 bytes from 10.20.22.254: icmp_seq=3 ttl=64 time=1.24 ms  
64 bytes from 10.20.22.254: icmp_seq=4 ttl=64 time=1.39 ms  
64 bytes from 10.20.22.254: icmp_seq=5 ttl=64 time=3.35 ms  
64 bytes from 10.20.22.254: icmp_seq=6 ttl=64 time=1.22 ms  
64 bytes from 10.20.22.254: icmp_seq=7 ttl=64 time=1.57 ms  
64 bytes from 10.20.22.254: icmp_seq=8 ttl=64 time=2.15 ms  
64 bytes from 10.20.22.254: icmp_seq=9 ttl=64 time=1.11 ms  
64 bytes from 10.20.22.254: icmp_seq=10 ttl=64 time=3.32 ms  
^C  
--- 10.20.22.254 ping statistics ---  
10 packets transmitted, 10 received, 0% packet loss, time 9098ms  
rtt min/avg/max/mdev = 1.113/1.820/3.351/0.804 ms
```

Examination of the DHCP Wireshark Capture

11. Which transport protocol is used in DHCP? (5 pts)

```
> Frame 51: 330 bytes on wire (2640 bits), 330 bytes captured (2640 bits) on interface -, id 0
> Ethernet II, Src: PcsCompu_0e:34:8d (08:00:27:0e:34:8d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Discover)
```

DHCP uses UDP.

12. What are the transport ports used in DHCP? (5 pts)

```
▼ User Datagram Protocol, Src Port: 68, Dst Port: 67
  Source Port: 68
  Destination Port: 67
  Length: 296
  Checksum: 0x72f5 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 2]
  > [Timestamps]
  UDP payload (288 bytes)
```

The source port is 68 and the destination port is 67.

13. Explain why the source machine has an IPv4 address of 0.0.0.0 during the DHCP Discover/Request phases. (5 pts)

The client starts out with an IPv4 address of 0.0.0.0 (default address) and then the server gives it a new IP address.

14. Explain why the destination machine has an IPv4 address of 255.255.255.255 during the DHCP Discover/Request phases. (5 pts)

255.255.255.255 is the default broadcast address which means that the client that has the 0.0.0.0 ip address will use it to find a DHCP server.

15. In the DHCP Offer packet, what is the IPv4 Address lease time? (5 pts) *Hint: located in the packet details's option 51*

```
▼ Option: (51) IP Address Lease Time
  Length: 4
  IP Address Lease Time: (3600s) 1 hour
```

The lease time is 1 hour.

bonus section:

Due: Thursday, February 17, 2022 @ 11:59 PM

Editing Wired connection 1

Connection name: Wired connection 1

General Ethernet 802.1X Security DCB Proxy **IPv4 Settings** IPv6 Settings

Method: Automatic (DHCP)

Additional static addresses

Address	Netmask	Gateway

Add

Delete

Additional DNS servers

Additional search domains

DHCP client ID

☐ Require IPv4 addressing for this connection to complete

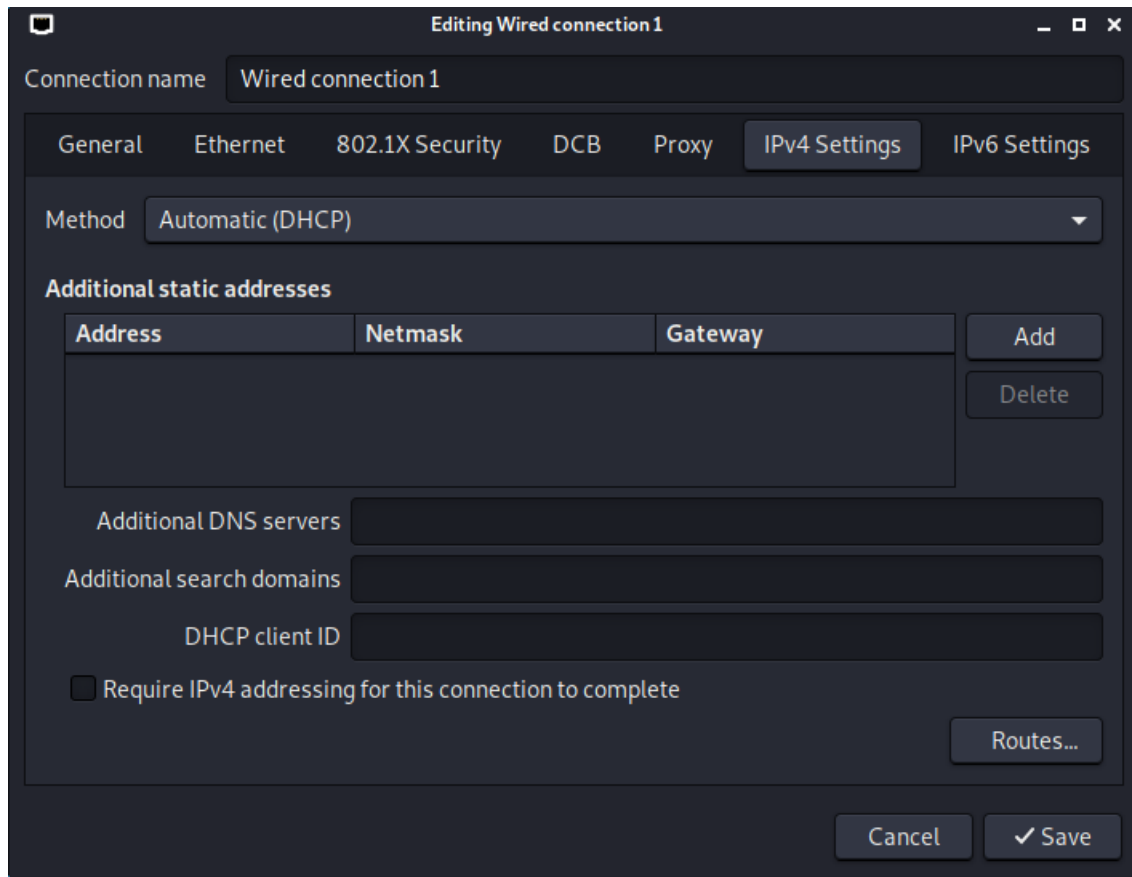
Routes...

Cancel Save

Setting the settings to automatic (dhcp) and deleting the old ip address. (Lubuntu)

=====

Due: Thursday, February 17, 2022 @ 11:59 PM



Setting the settings to automatic (dhcp) and deleting the old ip address. (Kali)

=====