Week 5 – Tutorial DHCP Configuration

Systems and Cyber Security

24_25

School of Computer Science and Digital Technologies

Contents

DHCP lab

Part 1

Dynamic Host Configuration Protocol is a protocol that helps in assigning IP Addresses and other essential IP related configurations like gateway and DNS addresses to devices on a network.

Assigning IP Addresses can be done in 2 main ways:

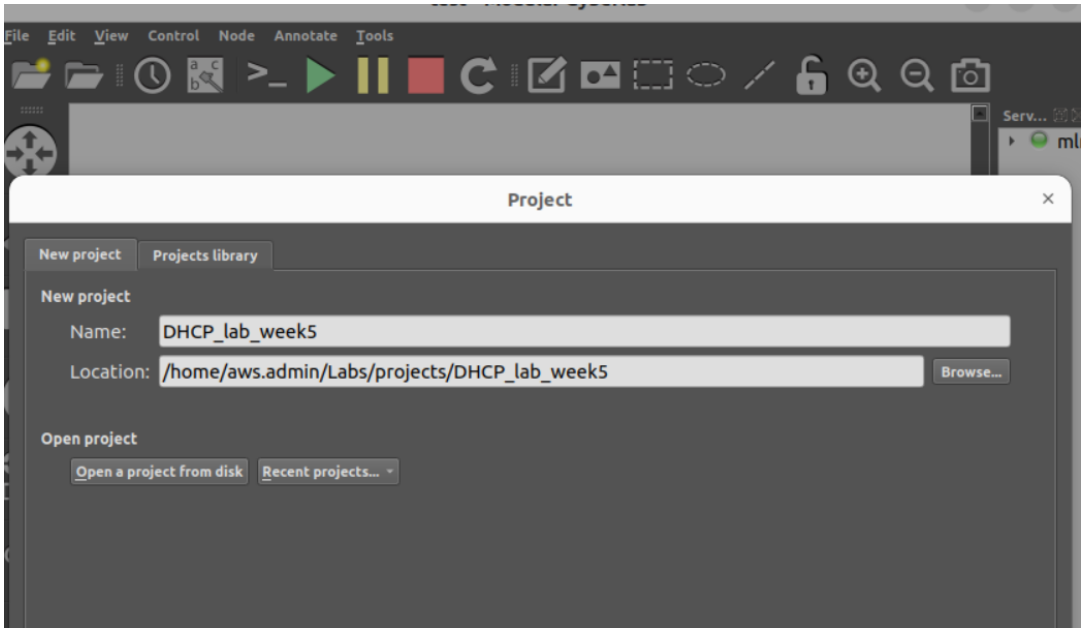
i. Statically
ii. Dynamically

Static IP Address assignment is done by going on a machine and allocating an IP Address on it.

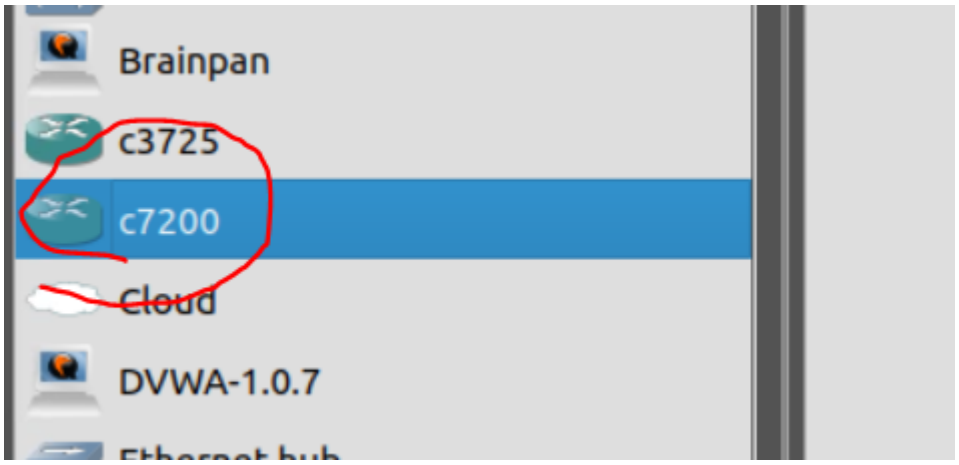
Dynamic IP Address assignment is done by allowing a server to offer an IP Address to a device that request for an IP address. This helps to reduce the burden of having to assign addresses manually and provide some of IP Address management since two devices will not be mistakenly assigned the same address. The DHCP server keeps a binding table that records the addresses and their lease period to ensure that no IP address is mistakenly reassigned to another device when in use.

In this lab will build a simple network and configure DHCP server on the router. This will ensure that every device that joins the network will have an IP address.

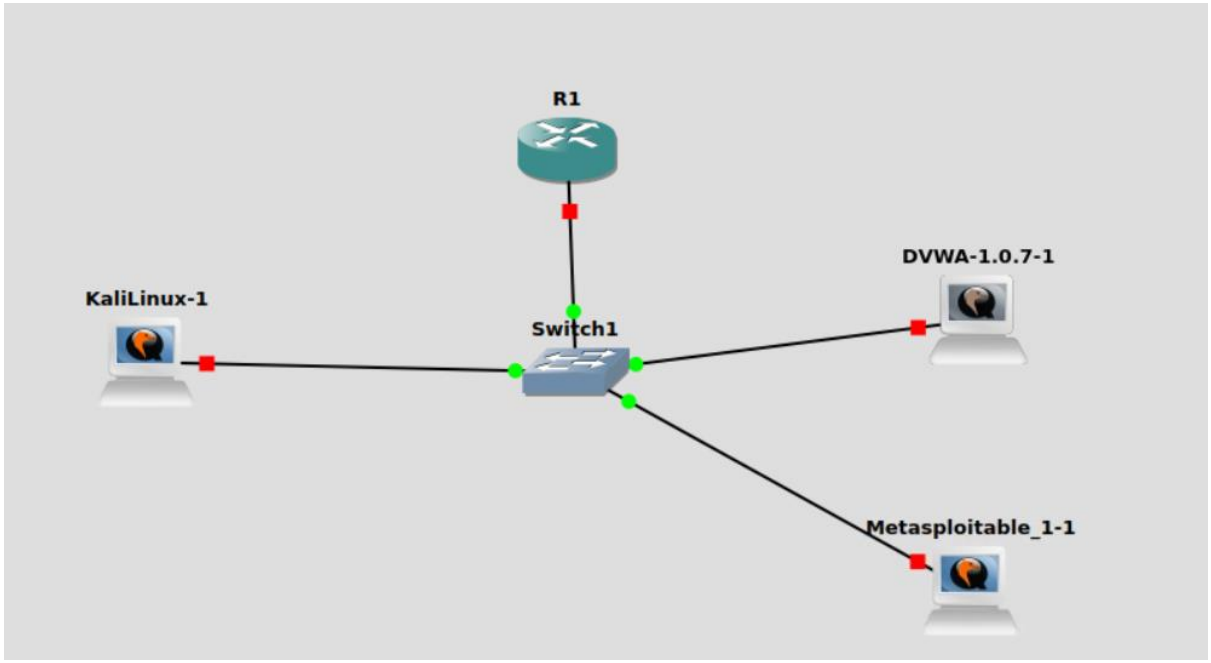
Step 1 – Create a new project and name it **DHCP_lab_week5**



Step 2 – Select the appropriate router c7200

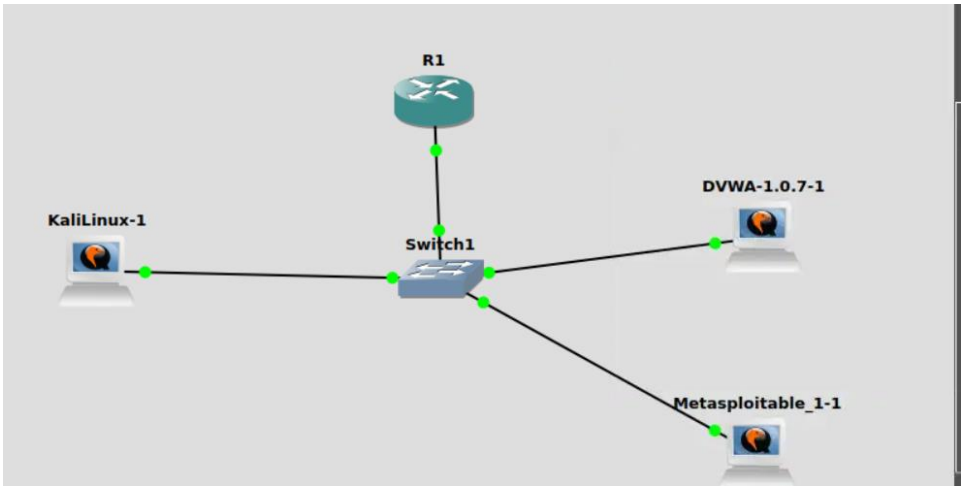


Step 3 – Ensure that all the relevant devices in the topology below are used for the design.



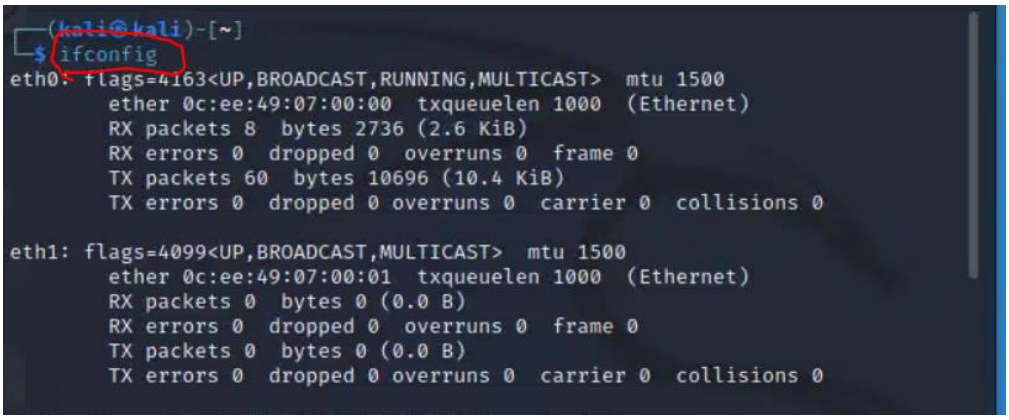
We will be assigning the **10.0.0.0/24** network which meanings the subnet mask is **255.255.255.0** . The router will be acting as the DHCP server and the gateway. We will allocate the first IP address to the router and that means no other device will be given the chance to request for the 10.0.0.1 address.

Step 4 – Ensure that the devices are started.



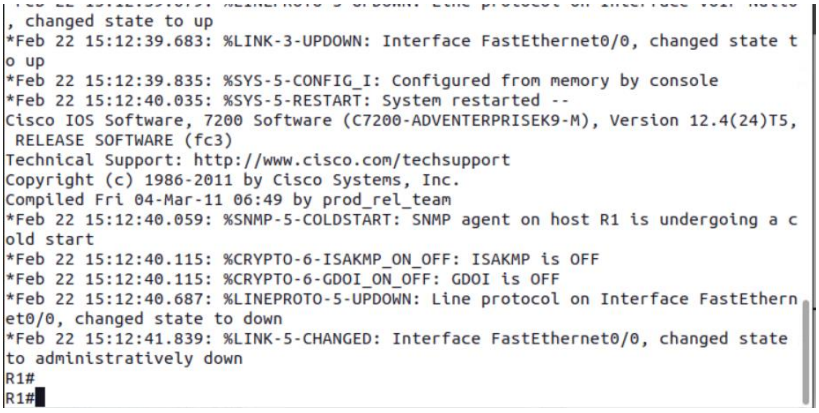
Step 5 – Check the IP configuration on the device.

It can be noticed that there is no IP Address assigned to the device. Do this check by using the **ifconfig** command



Step 6 – Configuring the router as the DHCP server

Go to the router console and similar view will be seen.



The router currently is in **enable mode**, and we will have to go to configuration mode to do some configuration to ensure that it will server as the DHCP server.

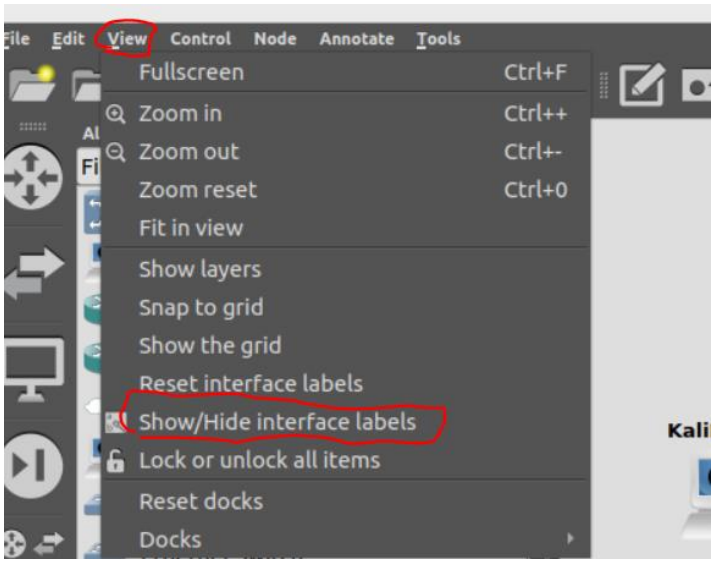
```
R1#
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#
```

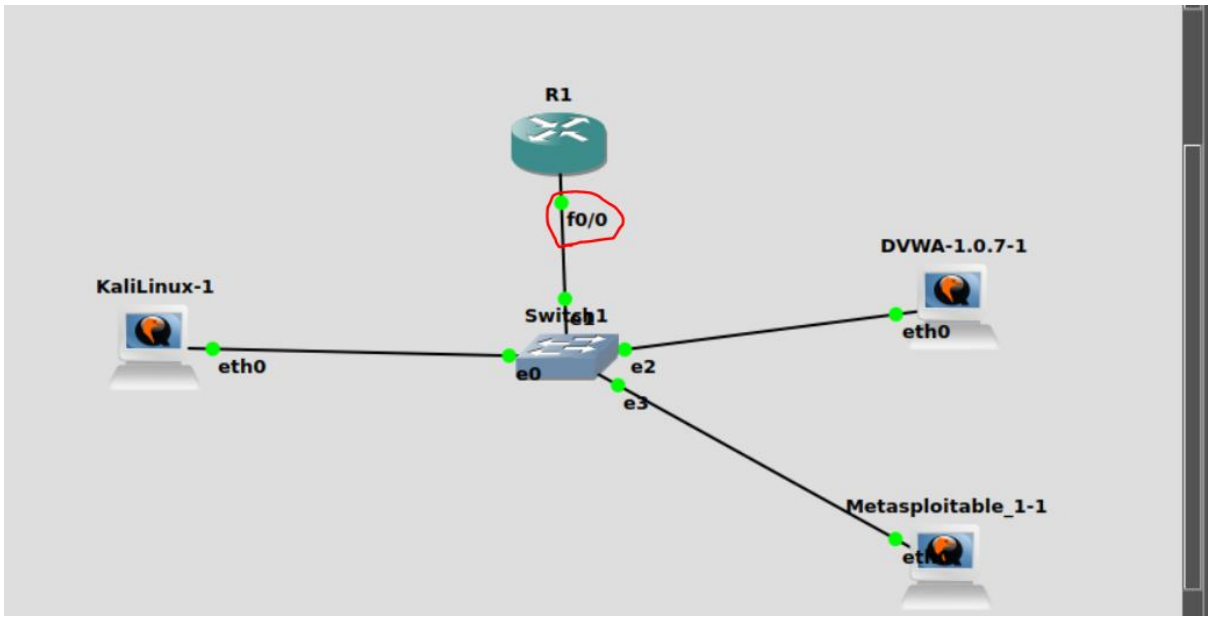
Type the command **configure terminal** and enter. It can be seen that there is a slight difference between the initial prompt before the command was sent and the current prompt.

Type the command **?** to see the various configurations that can be performed . Press the space bar to see more command and configurations that can be performed.

```
R1(config)#?
Configure commands:
  aaa                         Authentication, Authorization and Accounting.
  aal2-profile                Configure AAL2 profile
  access-list                 Add an access list entry
  alias                       Create command alias
  alps                        Configure Airline Protocol Support
  appfw                       Configure the Application Firewall policy
  appletalk                   Appletalk global configuration commands
  application                 Define application
  arap                        Appletalk Remote Access Protocol
  archive                     Archive the configuration
  arp                         Set a static ARP entry
  ase                         Configure ASE
  async-bootp                 Modify system bootp parameters
  auto                        Configure Automation
  backhaul-session-manager    Configure Backhaul Session Manager
```

```
identity                    Identity Configuration Commands
interface                   Select an interface to configure
ip                          Global IP configuration subcommands
ipc                         Configure IPC system
iphc-profile                Configure IPHC profile
ipv6                        Global IPv6 configuration commands
ipx                         Novell/IPX global configuration commands
isis                        Global ISIS configuration subcommands
ivr                         ivr utility command
ixi                         IXI Config command
kerberos                    Configure Kerberos
key                         Key management
keymap                      Define a new keymap
```





Will configure the router interface f0/0 with the IP address 10.0.0.1 and subnet mask 255.255.255.0 . To do this we need to type the command below.

NB if the interface id appearing on the router is different from what is above ensure to use that. So if you see f0/1 on the router interface, use the command int f0/1

```
R1(config)#int f0/0
R1(config-if)#
```

```
R1(config-if)#ip address 10.0.0.1 255.255.255.0
```

```
R1(config-if)#no shutdown
R1(config-if)#
*Feb 22 15:39:47.059: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*Feb 22 15:39:48.059: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
```

To configure the IP address on the interface you need to type the command ***ip address [ip_address subnet_mask]***. So, since we want to assign the IP address 10.0.0.1 and subnet mask 255.255.255.0, we will type the command **ip address 10.0.0.1 255.255.255.0** just like the image above

To save the configuration write the command below **do write memory**.

```
R1(config-if)#do write memory
Building configuration...
[OK]
```

```
R1(config-if)#exit
R1(config)#exit
R1#
*Feb 22 16:21:47.895: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

To see the current configuration on the device use the command **show run** or sh run

In the diagram below the command sh run was used and to see more of the configuration use the space bar on the keyboard to navigate down to more configurations.

```
R1#sh run
Building configuration...

Current configuration : 911 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
```

Step 8 – Configuring the router as DHCP server

DHCP Configuration

To configure the router as the DHCP server we will go back to the router and go to configuration mode. The command can be seen as below.

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

Since the interface f0/0 on the router has been configured with the IP address **10.0.0.1**, we exclude it in the DHCP pool of addresses to be assigned. This means that no device will be assigned the IP address **10.0.0.1**.

```
R1(config)#ip dhcp excluded-address 10.0.0.1
```

We will now create the DHCP pool of addresses. To do that we will type the **ip dhcp pool** command and give it a name and in this case, we want to refer to the pool as **NetworkPOOL .** The command will now be **ip dhcp pool NetworkPOOL**.

```
R1(config)#ip dhcp pool NetworkPOOL
R1(dhcp-config)#
```

Now we will assign IP address pool with the command below.

```
R1(dhcp-config)#network 10.0.0.0 255.255.255.0
R1(dhcp-config)#
```

From the command above the network **10.0.0.0** with subnet mask **255.255.255.0** has been configured in the pool **NetworkPOOL**.

As mentioned in the introduction, DHCP server can also provide some extra information apart from the IP address . In the configuration below we are adding the default gateway and the IP address of the DNS server all being the IP address of the router. This means that if the devices that receive the IP address from the DHCP server will want to go outside the network the first hop will be the router, since the **10.0.0.1** address points to the interface **f0/0** on the router.

```
R1(dhcp-config)#default-router 10.0.0.1
R1(dhcp-config)#dns-server 10.0.0.1
R1(dhcp-config)#exit
```

Now save the command by doing **do write memory**.

```
R1(config)#do write memory
Building configuration...
[OK]
```

Now let us scan the network and see if there are any live hosts and get their IP Addresses.

```
R1(config)#exit
R1#
*Feb 22 16:52:19.335: %SYS-5-CONFIG_I: Configured from console by console
R1#sh run
Building configuration...

Current configuration : 1058 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
```

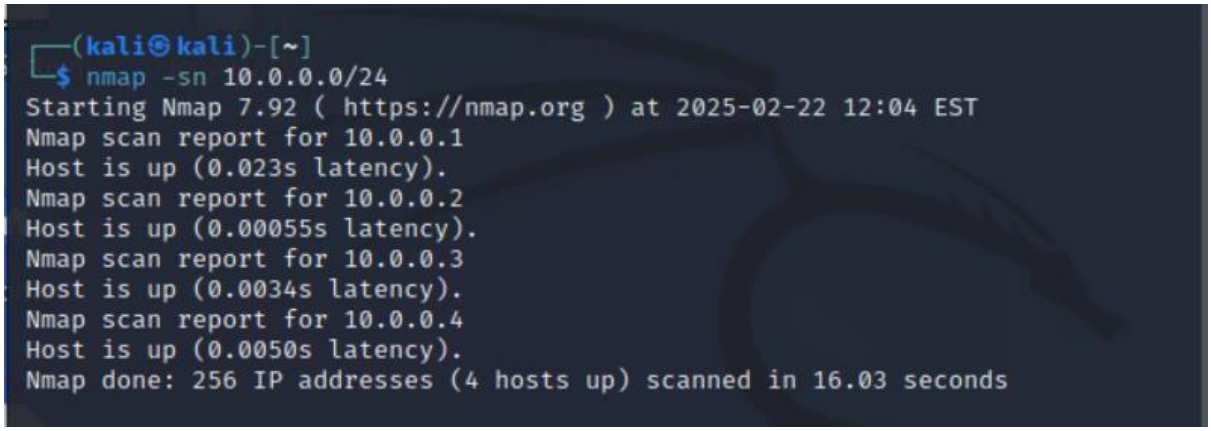
Scroll down in the configuration and the information about DHCP configurations will be seen.

```
!
!
ip dhcp excluded-address 10.0.0.1
!
ip dhcp pool NetworkPOOL
   network 10.0.0.0 255.255.255.0
   default-router 10.0.0.1
   dns-server 10.0.0.1
!
```

Go back to the Kali and run the ifconfig command in the terminal and you will see that the device has been given an IP address from the pool of addresses that were configured. Notice that the device was not given **10.0.0.1** but rather **10.0.0.2**

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.2  netmask 255.255.255.0  broadcast 10.0.0.255
        inet6 fe80::eee:49ff:fe07:0  prefixlen 64  scopeid 0x20<link>
        ether 0c:ee:49:07:00:00  txqueuelen 1000  (Ethernet)
        RX packets 100  bytes 24214 (23.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 204  bytes 35207 (34.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

It may be a different number on yours if you have multiple devices on the network also it can be seen that the subnet mask is **255.255.255.0** as configured on the DHCP server.



Using the Nmap command above there are other hosts on the network and apart from our Kali. There are 3 more hosts since we configured the router with **10.0.0.1**, we can be sure that the other devices are **10.0.0.3** and **10.0.0.4** .

Part 2

Do the following exercises

i. Check what services are running on the various nodes
ii. Check the Operating systems running on them
iii. What versions of the services and Operating systems are running on them?
iv. If any of the systems are running a web application, test the application in the browser.
v. From the services running are there any security implications.
vi. Recommend any mitigation strategies that can be implemented to reduce such risk from occurring.