**Homework 2** Shruti Soni

Task: **Find out all IP connected live to current network through Linux Kali**

In this method nmap is useful to find the IP of connected devices

The [Nmap](https://www.tecmint.com/nmap-command-examples/" \t "_blank) (short form for **Network Mapper**) is an open source, powerful and a very versatile command line tool for exploring networks, [perform security scans, network audit](https://www.tecmint.com/audit-network-performance-security-and-troubleshooting-in-linux/) and [finding open ports on remote machine](https://www.tecmint.com/find-open-ports-in-linux/) and so much more.

Commands:

Subnet mask

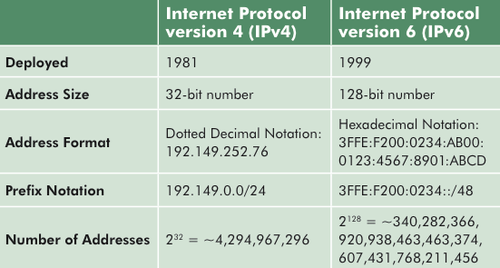
>>ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  
        inet 172.22.9.31  netmask 255.255.254.0  broadcast 172.22.9.255  
        inet6 fe80::ed22:c319:c758:cbdc  prefixlen 64  scopeid 0x20<link>  
        ether 98:90:96:e1:0e:c9  txqueuelen 1000  (Ethernet)  
        RX packets 80148  bytes 75824239 (72.3 MiB)  
        RX errors 0  dropped 0  overruns 0  frame 0  
        TX packets 57182  bytes 9189482 (8.7 MiB)  
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0  
        device interrupt 20  memory 0xf7c00000-f7c20000    
  
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536  
        inet 127.0.0.1  netmask 255.0.0.0  
        inet6 ::1  prefixlen 128  scopeid 0x10<host>  
        loop  txqueuelen 1  (Local Loopback)  
        RX packets 16  bytes 876 (876.0 B)  
        RX errors 0  dropped 0  overruns 0  frame 0  
        TX packets 16  bytes 876 (876.0 B)  
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

Ipv6

Ipv4

Now first should learn difference between **ipv4 and ipv6**



Second should learn **classful and classless** routing:

Classful is based on the default Class A,B or C networks.

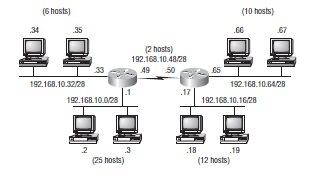
- Class A: 0 - 127 with a mask of 255.0.0.0 (/8)

- Class B: 128 - 191 with a mask of 255.255.0.0 (/16)

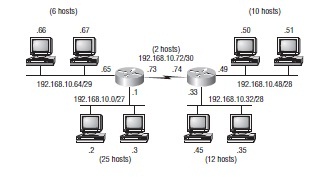
- Class C: 192 - 223 with a mask of 255.255.255.0 (/24)

All devices in the same routing domain must use the same subnet mask

A classful network uses IP addresses of the same network class in all its sub-networks and in addition, the same subnet mask in all the subnets (i,e if class A, all the IP addresses in the network are of class A)

[](https://learningnetwork.cisco.com/servlet/JiveServlet/showImage/2-178096-58835/classful.jpg)

Classless networks enable the use of IP addresses with different subnet masks in the same network to enable efficient use of IP addresses

[](https://learningnetwork.cisco.com/servlet/JiveServlet/showImage/2-178096-58836/classless.jpg)

#### CIDR notation

The **Classless Inter-domain Routing**(**CIDR**) notation (pronounced cider) is a compact method for specifying IP addresses and their routing suffixes. This notation gained popularity due to its granularity when compared with classful addressing because it allows subnet masks of variable length.

The CIDR notation is specified by an IP address and network suffix. The network or IP suffix represent the number of network bits. IPv4 addresses are 32 bit, so the network can be between 0 and 32. The most common suffixes are /8, /16, /24, and /32.

To visualize it, take a look at the following CIDR-to-Netmask conversion table:

|  |  |
| --- | --- |
| CIDR | Netmask |
| /8 | 255.0.0.0 |
| /16 | 255.255.0.0 |
| /24 | 255.255.255.0 |
| /32 | 255.255.255.255 |

For example, 192.168.1.0/24 represents the 256 IP addresses from 192.168.1.0 to 192.168.1.255

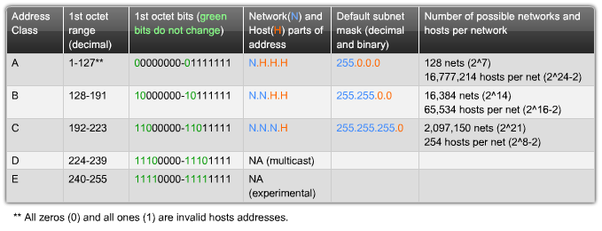
(Source from: <https://www.packtpub.com/mapt/book/networking_and_servers/9781786467454/1/ch01lvl1sec16/scanning-an-ip-address-ranges>, <https://learningnetwork.cisco.com/thread/34420> )

Third should learn how to define **class of IP:**

Example my ip is : 172.22.9.00

So it starts from 172: 128 64 32 16 8 4 2 1

1 0 1 0 1 1 0 0



So in above example bit starts from the 1 0 which format Is similar to the class B so we can define the above ip is class B address .

Then what is subnet: borrow bits from the host section of class called subnet

it will work increase no of network and decrease host

-Same network , on same subnet so

Why have to use subnet :

Example:

my IP: 172.22.9.31

Mask: 255.255.254.0 == 8+8+7+0 because (X AND 255 =X)

 255=1111 1111 255=1111 1111 254: 1111 1110 0= 0000 0000

172=1010 1100    22= 0001 0110   9:  0000 1001 31=

-----------------------------------------------------------------------------------------

 1010 1100 0001 0110 0000 1000 0000 0000 / 8+8+7+0 /left over 1+8

172 22 8 0 / 23 bit / left over =9 bit

Subnet address: 172.22.8.0

1 network address: 172.22.8.0

2. Broadcast address: 172.22.9.255

3. First host address: 172.22.8.1 (NA+1)

4. Last host address 172.22.9.254(BA-1)

## **Scan a network and find out which servers and devices are up and running**

This is known as host discovery or ping scan (Gite, 2012):

How we get the network address: Application --> information gathering--> nmap

>>nmap -nsP 172.22.8.0/23

Nmap= network mapper ping scan

So, Total lab 3 work is focus on the how to calculate the network address using the AND operator

Now Lab 4 work is find total number of ip connected to the network

send the output to (scan 510 devices)

>>nmap -sP 172.22.8.0/23 > myip.txt

How to print the file value :

>>less myip.txt

(We need IP + Mac address : )

Output should be this:

Extrect ip adress -->>head -n 6 myip.txt

Starting Nmap 7.40 ( https://nmap.org ) at 2017-09-16 15:42 UTC  
Nmap scan report for 172.22.8.1  
Host is up (0.0072s latency).  
MAC Address: 00:18:B9:37:4F:C7 (Cisco Systems)  
Nmap scan report for 172.22.8.60  
root@kali:~# grep for myip.txt  
Nmap scan report for 172.22.8.1  
Nmap scan report for 172.22.8.60  
Nmap scan report for 172.22.8.61  
Nmap scan report for 172.22.8.62  
Nmap scan report for 172.22.8.63  
Nmap scan report for 172.22.8.100  
Nmap scan report for 172.22.8.102  
Nmap scan report for 172.22.8.103  
Nmap scan report for 172.22.8.113  
Nmap scan report for sch563-d02.roosevelt.edu (172.22.9.1)  
Nmap scan report for 172.22.9.2  
Nmap scan report for schmpc-m07.roosevelt.edu (172.22.9.3)  
Nmap scan report for 172.22.9.4  
Nmap scan report for sch523-l01.roosevelt.edu (172.22.9.5)  
Nmap scan report for sch504-l18.roosevelt.edu (172.22.9.6)  
Nmap scan report for student-pc.roosevelt.edu (172.22.9.8)  
Nmap scan report for sch515-l20.roosevelt.edu (172.22.9.9)  
Nmap scan report for sch504-l02.roosevelt.edu (172.22.9.10)  
Nmap scan report for sch504-l23.roosevelt.edu (172.22.9.11)  
Nmap scan report for sch525-l01.roosevelt.edu (172.22.9.12)  
Nmap scan report for 172.22.9.13  
Nmap scan report for sch504-l19.roosevelt.edu (172.22.9.14)  
Nmap scan report for sch504-l21.roosevelt.edu (172.22.9.15)  
Nmap scan report for sch504-l01.roosevelt.edu (172.22.9.16)  
Nmap scan report for sch504-l10.roosevelt.edu (172.22.9.17)  
Nmap scan report for sch515-l09.roosevelt.edu (172.22.9.18)  
Nmap scan report for sch504-l03.roosevelt.edu (172.22.9.19)  
Nmap scan report for sch504-l11.roosevelt.edu (172.22.9.20)  
Nmap scan report for 172.22.9.21  
Nmap scan report for sch515-l18.roosevelt.edu (172.22.9.22)  
Nmap scan report for 172.22.9.23  
Nmap scan report for sch504-l15.roosevelt.edu (172.22.9.24)  
Nmap scan report for sch554-d01.roosevelt.edu (172.22.9.25)  
Nmap scan report for 172.22.9.27  
Nmap scan report for sch504-l25.roosevelt.edu (172.22.9.28)  
Nmap scan report for sch515-l01.roosevelt.edu (172.22.9.29)  
Nmap scan report for sch504-l22.roosevelt.edu (172.22.9.30)  
Nmap scan report for 172.22.9.32  
Nmap scan report for 172.22.9.33  
Nmap scan report for sch532-d01.roosevelt.edu (172.22.9.35)  
Nmap scan report for sch515-l24.roosevelt.edu (172.22.9.36)  
Nmap scan report for sch515-l19.roosevelt.edu (172.22.9.38)  
Nmap scan report for sch515-l06.roosevelt.edu (172.22.9.39)  
Nmap scan report for sch504-l17.roosevelt.edu (172.22.9.40)  
Nmap scan report for 172.22.9.42  
Nmap scan report for sch515-l17.roosevelt.edu (172.22.9.43)  
Nmap scan report for sch504-l12.roosevelt.edu (172.22.9.46)  
Nmap scan report for 172.22.9.47  
Nmap scan report for sch812-lt380 (172.22.9.48)  
Nmap scan report for sch504-l20.roosevelt.edu (172.22.9.50)  
Nmap scan report for sch504-l23.roosevelt.edu (172.22.9.51)  
Nmap scan report for 172.22.9.207  
Nmap scan report for 172.22.9.208  
Nmap scan report for 172.22.9.209  
Nmap scan report for sch504-l14.roosevelt.edu (172.22.9.210)  
Nmap scan report for sch515-l07.roosevelt.edu (172.22.9.211)  
Nmap scan report for sch504-l07.roosevelt.edu (172.22.9.212)  
Nmap scan report for sch552-l01.roosevelt.edu (172.22.9.214)  
Nmap scan report for sch504-l08.roosevelt.edu (172.22.9.215)  
Nmap scan report for sch504-l24.roosevelt.edu (172.22.9.217)  
Nmap scan report for sch558-l01.roosevelt.edu (172.22.9.221)  
Nmap scan report for 172.22.9.31  
root@kali:~#   
(Retrive the head lines)  
  
>>grep for myip.txt | cut -d' ' -f5   
>>grep for myip.txt | cut -d' ' -f5-6

root@kali:~# nmap -nsP 172.22.8.0/23 > myip.txt  
root@kali:~# grep 172 myip.txt | cut -d' ' -f5

172.22.8.1  
172.22.8.60  
172.22.8.61  
172.22.8.62  
172.22.8.63  
172.22.8.100  
172.22.8.102  
172.22.8.103  
172.22.8.113  
172.22.9.1  
172.22.9.2  
172.22.9.3  
172.22.9.4  
172.22.9.5  
172.22.9.6  
172.22.9.8  
172.22.9.9  
172.22.9.10  
172.22.9.11  
172.22.9.12  
172.22.9.13  
172.22.9.14  
172.22.9.15  
172.22.9.16  
172.22.9.17  
172.22.9.18  
172.22.9.19  
172.22.9.20  
172.22.9.21  
172.22.9.22  
172.22.9.23  
172.22.9.24  
172.22.9.25  
172.22.9.27  
172.22.9.28  
172.22.9.29  
172.22.9.30  
172.22.9.32  
172.22.9.33  
172.22.9.35  
172.22.9.36  
172.22.9.38  
172.22.9.39  
172.22.9.40  
172.22.9.42  
172.22.9.43  
172.22.9.46  
172.22.9.47  
172.22.9.48  
172.22.9.50  
172.22.9.51  
172.22.9.207  
172.22.9.208  
172.22.9.209  
172.22.9.210  
172.22.9.211  
172.22.9.212  
172.22.9.214  
172.22.9.215  
172.22.9.217  
172.22.9.221  
172.22.9.31

root@kali:~# grep 172 myip.txt | cut -d' ' -f5 >ips.txt  
root@kali:~#

command:   
>> nmap -nsP 172.22.8.0/23 > myip.txt

root@kali:~# grep 172 myip.txt | cut -d' ' -f5 >ips.txt

grep MAC myip.txt | cut -d' ' -f3

Total Used commands :-🡪

>>nmap -nsP 172.22.8.0/23 > myip.txt  
>>grep 172 myip.txt | cut -d' ' -f3 > ips.txt  
>>grep MAC myip.txt | cut -d' ' -f3 > mac.txt  
>>paste ips.txt mac.txt > cst\_390\_460\_soni\_shruti.txt  
>>wc -l filename.txt : will show how many line u have in file

# References

Gite, V. (2012, November 26). *Top 32 Nmap Command Examples For Sys/Network Admins*. Retrieved from cyberciti: https://www.cyberciti.biz/networking/nmap-command-examples-tutorials/

<https://www.packtpub.com/mapt/book/networking_and_servers/9781786467454/1/ch01lvl1sec16/scanning-an-ip-address-ranges>

<https://learningnetwork.cisco.com/thread/34420>