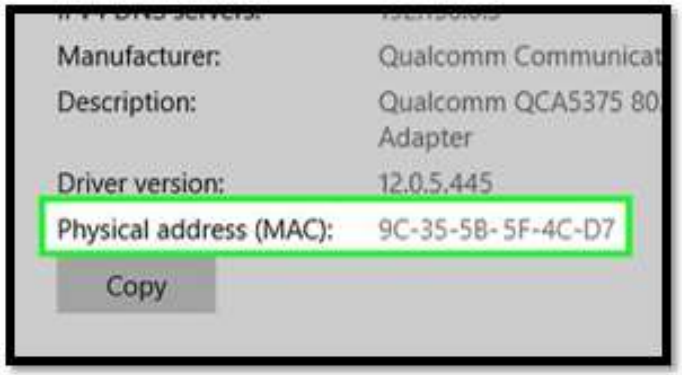
Network Scanner

By- Prashant Ranjan Singh

To do

- ✓ **Discover all devices on the network**



- ✓ **Find there IP address (internal)**
- ✓ **Find there Mac Address**

Basic of Network

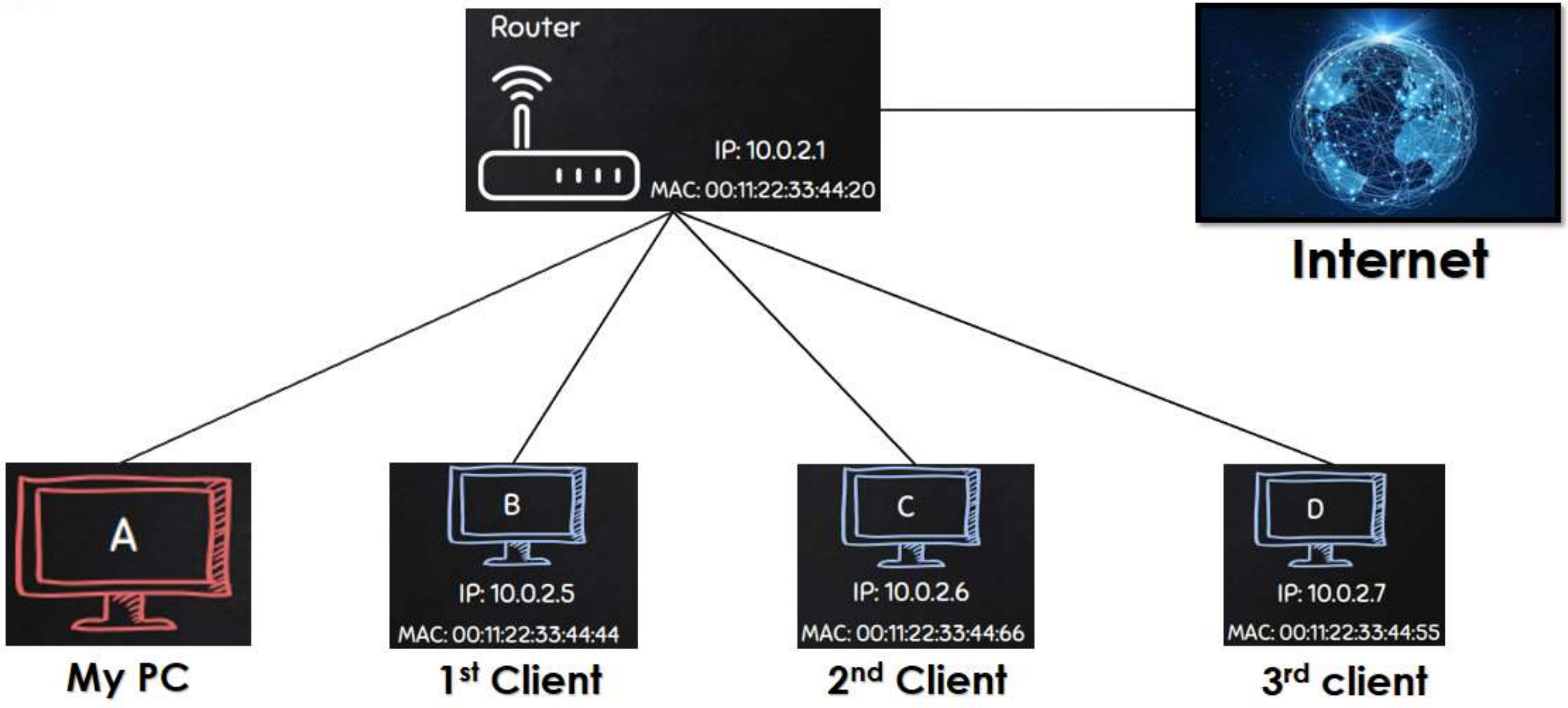
- All Device communicate inside the network with there Mac Address
- Maximum amount of device which can connect to a router (Wi-Fi, Wired + Wi-Fi, Wired) is 256.
- This is how an internal IP address look like 192.168.29.57 so all the device connected to same network will have this part same “192.169.29”.
- And all the device which connect to that network will have ip address between

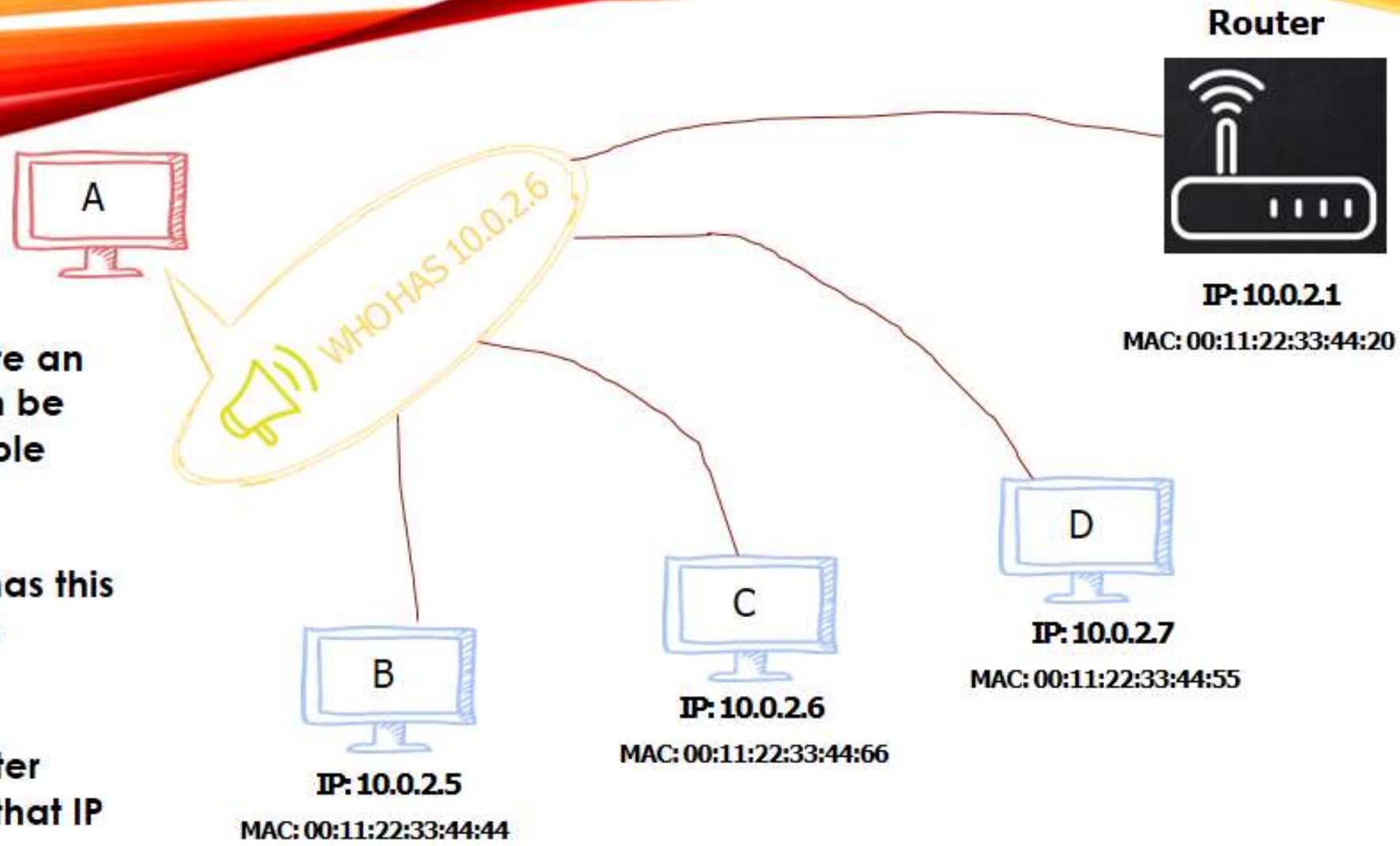
  192.168.29.1 – 192.168.29.254 (including Router).

Note

- If we send any date packet outside for this network (example- www.google.com) so google server can only knows the external ip address not are internal ip address
- For example if we type what is my ip on google it will show “ipv4 or ipv6” address but that address will not our internal ip address.
- you can see it practically by typing what is my Ip address from 2 device connected to same router it will show same ip address until and unless you connected to different Network, try it out once.

Normal Network without firewall, IDS, IPS

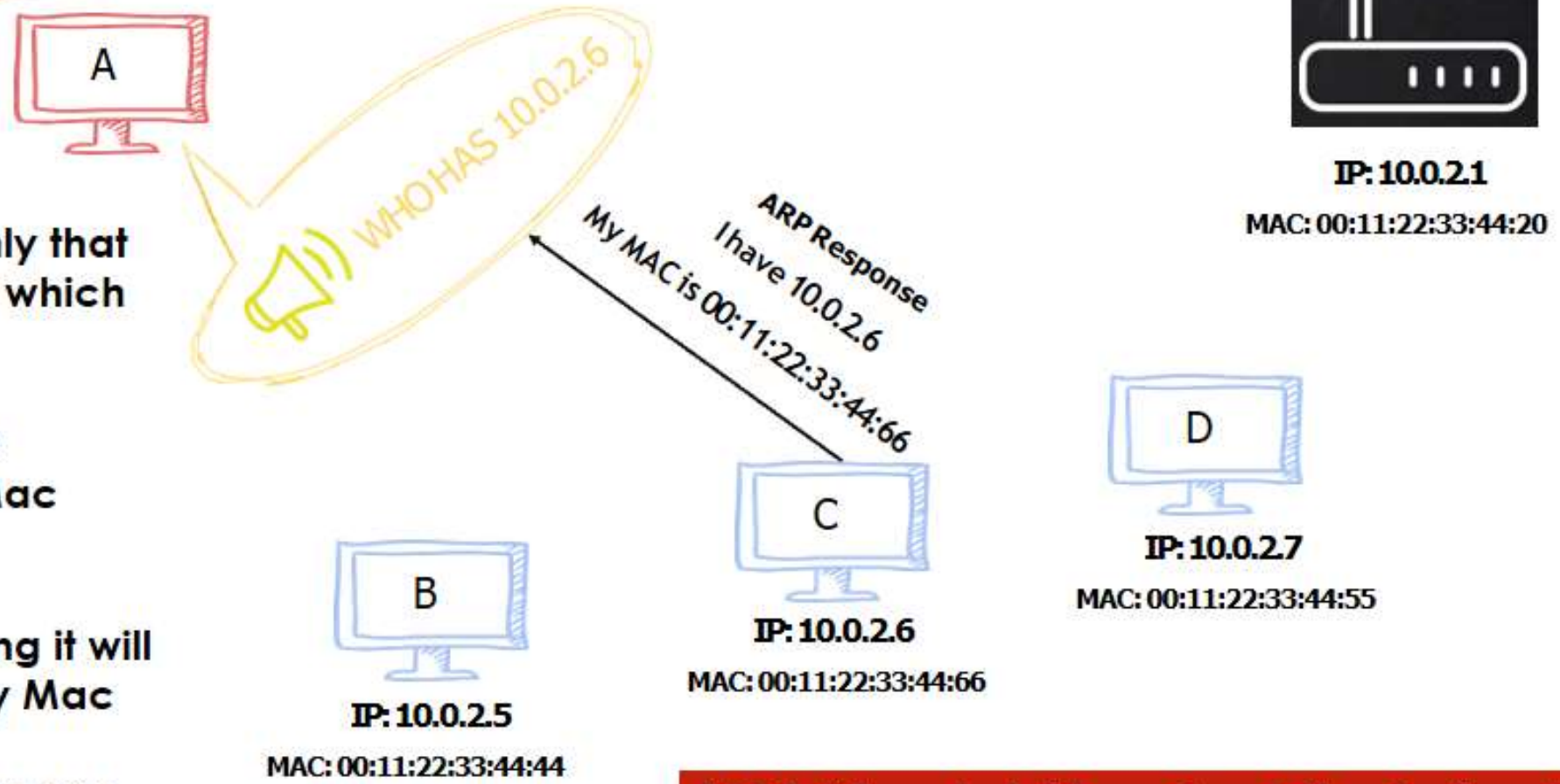




Our program will create an ARP packet which can be explained in most simple word as:

- It will ask that who has this IP address example 10.0.2.6
- So only that computer respond which has that IP Address
- Rest all devices will drop that request.

ARP is protocol which is used to change IP address into Mac Address by passing ARP packet to that device.



- As shown in slide only that device will respond which has that IP Address
- In this ARP response packet it will give Mac Address of it.
- Just for understanding it will say I am 10.0.2.6 my Mac Address is 00:11:22:33:44:66 you can communicate through it.

ARP full form is Address Resolution Protocol how this ARP packet convert IP address into Mac Address isn't explain in this ppt we use ARP protocol to find mac address has been explained.

Logic of the Program

- Now if we think about it a little bit we might strike a thought that, that ARP packet contains only 1 ARP packet which consist only 1 IP address so if we broadcast that ARP packet inside the network then if any device contain that IP address will respond it with its Mac Address.
- So as I explained in basic of network through 1 router only 256 device can connect so we will share 256 ARP packets b/w “nn:nn:nn:1 – nn:nn:nn:256”
- If that IP address present in the network then it will respond it with its mac address and other will drop that request.
- And if no ARP respond wont come then that device wont present in that network
- And we will capture that request and present it in list.

Requirement

- We need python3 install in our system
- We can install python by its official site and then install .deb or .rpm file in (Linux)
- We also need pip to be installed in our system so we can install library.
- For that write this command in terminal

  Command - sudo apt update && sudo apt upgrade && sudo apt get-install pip install
- We need to install a library for this program so type this command in terminal

  Command – sudo apt-get install pyhon-scapy

Optional

- Install PyCharm from its official site and install it so we can view code easly orr we can use notepad++ or visual code or any text editer to view the source of my file

Algorithm

STEPS

1. Create ARP request directed to broadcast MAC asking for IP.
2. Send packet and receive response.
3. Parse the response.
4. Print result.

GOAL

- To discover all devices connected to a network.

Explanation of Program

Library Used

1st – optparse

It is used to take arguments and value after python program like an social engineering tool.
For example --help to find how this program work

2nd – subprocess

It is used to pass system commands in terminal (in linux) or powershell (in windows)

3rd – scapy

It has lot of use related to network but in this program it is used to :-

- ✓ It is used to create ARP packet
- ✓ Add custom ether layer (broadband mac address)
- ✓ Record the response and store it in custom variable.

Thank You