Proyecto Final

Roberto Herrera

Curso Básico de Python

Nombre del Proyecto:

# Scanner de Redes con Python

Roberto Carlos Herrera

Estudiante

Enero 2025

## Contents



# Objetivo:

Utilizar todos los elementos de Lenguaje Python estudiados en clase:

- Variables
- Operadores lógicos y aritméticos
- Listas
- Diccionarios
- Iteraciones con While True
- Iteraciones con For
- Caracteres de Escape
- Funciones para dividir el programa en segmentos.

Para realizar un programa que escanee la red local donde se ejecute el mismo. Con fines educativos. El escaneo incluirá direcciones ip guardadas en listas al igual que direcciones MAC.

Luego se hizo el mismo ejercicio para guardarlos en diccionario utilizando la clave valor ip:valor y mac:valor guardando cada resultado en una lista.

## Complejidad:

El proyecto utilizo los elementos anteriormente descritos, pero se utilizo la librería scapy ya que se utilizada para redes. Por lo que el estudiante tiene que tener conceptos básicos de redes como:

- Protocolo
- Direccion IP
- Direccion física o MAC Address
- Red
- Mascara de Red

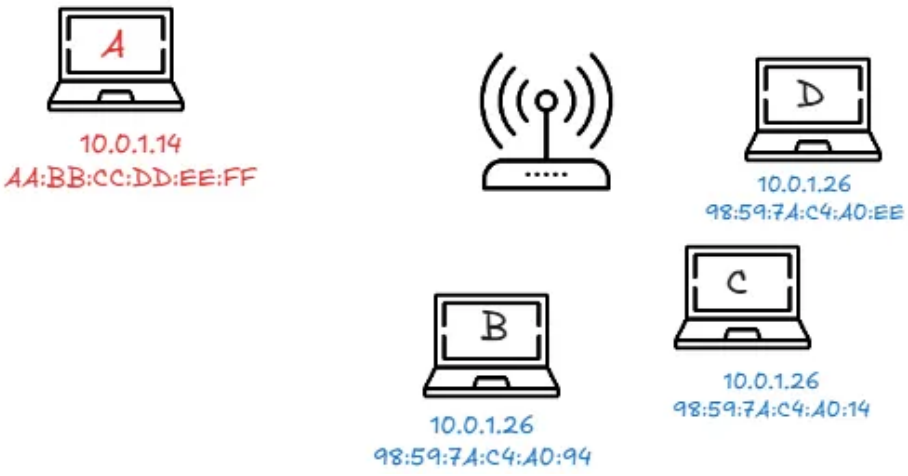
# Conceptos básicos de Protocolo ARP

## Conceptos básicos de redes

Hay varias formas de encontrar dispositivos en la misma red, la forma mas sencilla es replicar lo que haría un dispositivo normal para descubrir otro dispositivo en la misma red.

Por ejemplo si tenemos una red con dispositivos A B C D todos están en la misma red conectados a través de un Router.

Podemos ver que cada dispositivo tiene una dirección ***IP y una dirección MAC.***




Y supongamos que el dispositivo *A necesita comunicarse con el dispositivo C*.

Ahora también vamos a suponer que el dispositivo A conoce la IP del dispositivo C, pero como sabemos hasta ahora, para que estos dispositivos se comuniquen dentro de la misma red, A--> necesita conocer la dirección MAC del dispositivo C porque como dijimos antes, la comunicación dentro de la red se realiza utilizando la dirección Mac y NO utilizando la dirección IP. La direccion IP solo es un label, la direccion MAC es fija y fisica.

Ahora, lo que el dispositivo A haría es usar un protocolo llamado ARP para comunicarse.

ARP son las siglas de ***Address Resolution Protocol*** (protocolo de resolución de direcciones).

Y es un protocolo muy sencillo que nos permite vincular direcciones IP a direcciones MAC.

Así que el objetivo de este protocolo es ayudar en la situación donde un cliente necesita comunicarse con otro cliente. Donde solo Conoce la IP del otro cliente, pero no la dirección MAC.

Por lo que la computadora origen hace uso del protocolo ARP para identificar dicha dirección.

¿Como lo hace? Básicamente envía un mensaje de difusión, o sea, envía una solicitud ARP a una dirección MAC específica ***que SI conoce*** en toda la red, y a esta se conoce como la **dirección Broadcast Mac**.

---

Entonces se configura un paquete(trama de información) para que se envíe a la dirección Mac de difusión (Broadcast MAC), automáticamente todos los clientes de la misma red recibirán este paquete.

Entonces, ¿el dispositivo A enviará la difusión a todos los clientes de la red diciendo **¿Quién tiene la dirección 10.0.2.6?**

¡Este paquete va a ser dirigido a la dirección Mac Broadcast y por lo tanto todos los clientes de la red recibirán este paquete, este es un ejemplo de un ARP REQUEST!

Ahora todos estos dispositivos recibirán el paquete pero como no es para ellos, lo ignorarán excepto el que tiene esta dirección IP, que es 10.0.2.6, correspondiente al dispositivo C.

Así que, todos los dispositivos no harán nada, y el único dispositivo que responderá es el dispositivo C enviando una respuesta ARP.

El dispositivo C va a decir **YO TENGO LA 10.0.2.6. Y MI MAC ADDRESS ES 00:11:22:33:44:66**

De esta forma el dispositivo A tendrá la dirección Mac del dispositivo C y ahora podrá comunicarse con el dispositivo C y hacer cualquier tarea que quisiera hacer.

Así que toda esta comunicación se facilita utilizando el protocolo ARP.

Lo ves, el protocolo ARP es un protocolo muy sencillo.

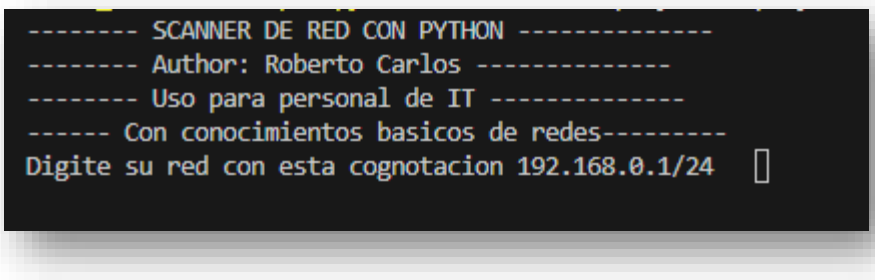

## Código fuente

Se puede obtener el código desde

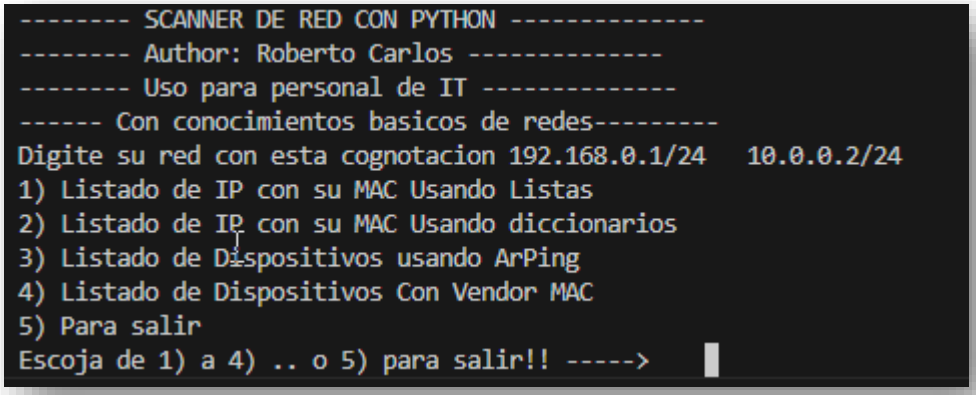
https://github.com/soportemicrosis/scannerconpython

## Ejecución del programa (imágenes)

SE SOLICITA LA IP DEL ROUTER CON SU SUBMASCARA /24

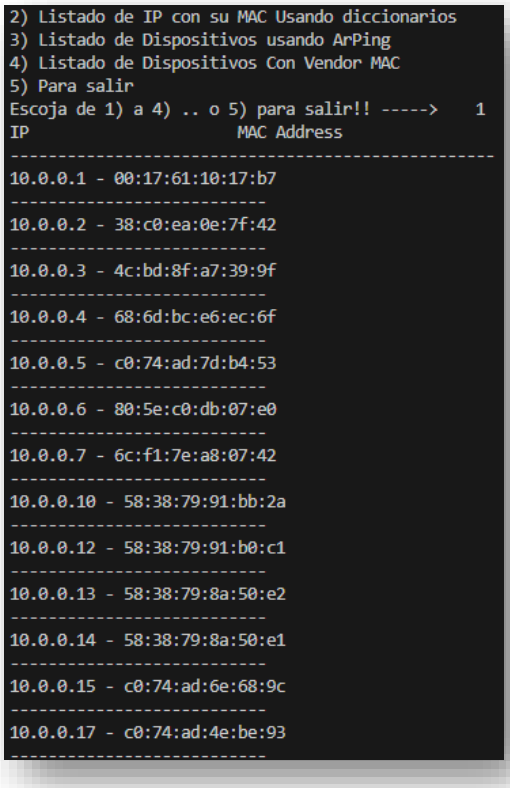


MENU PRINCIPAL



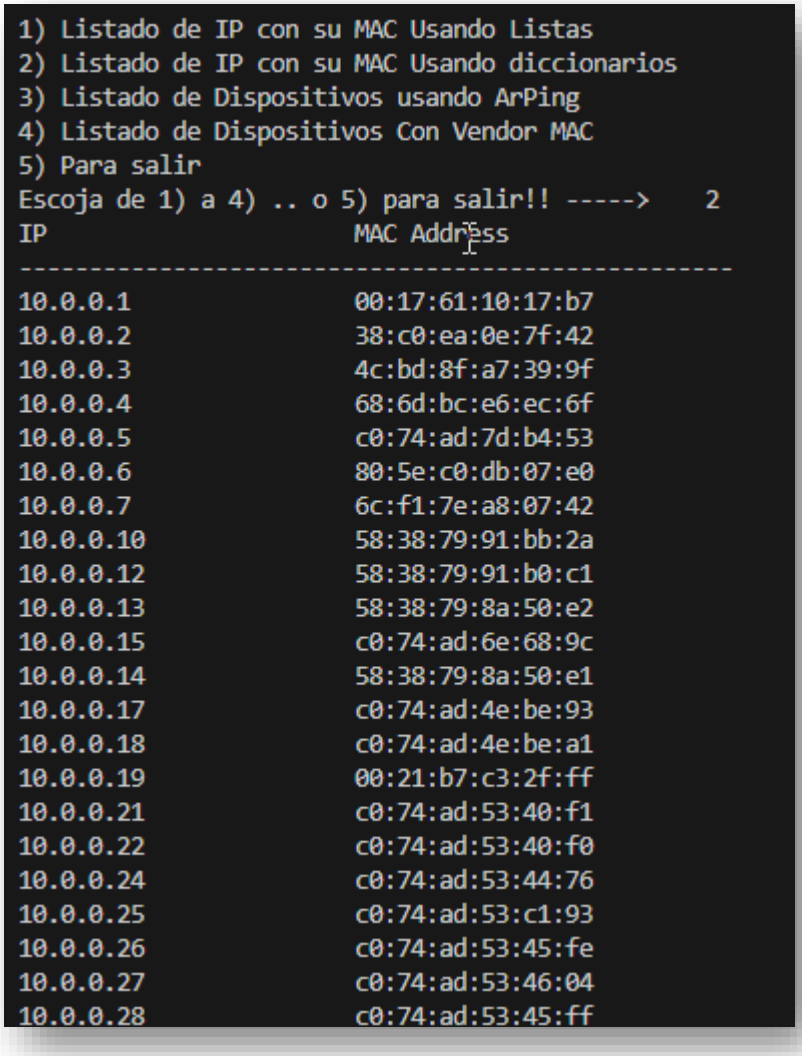

OPCION 1:

LISTADO DE DISPOSITIVOS CON IP Y MAC ADDRESS USANDO LISTAS



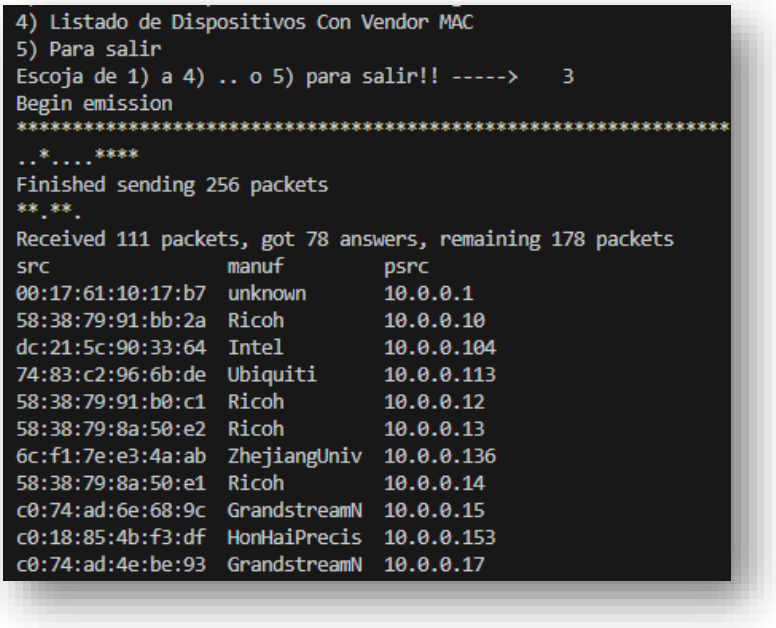
OPCION 2:

LISTADO DE DISPOSITIVOS CON IP Y MAC ADDRESS USANDO DICCIONARIOS



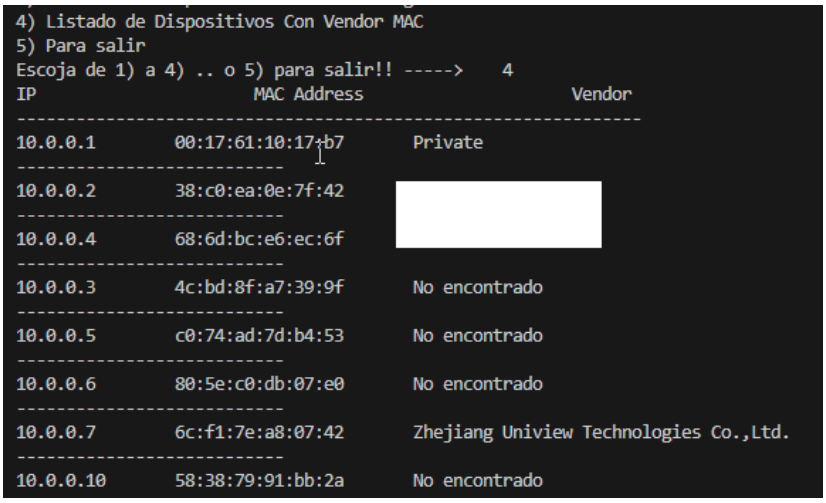
OPCION 3:

LISTADO DE DISPOSITIVOS SIMPLEMENTE USANDO LA LIBRERÍA CON SU FUNCION ARPING

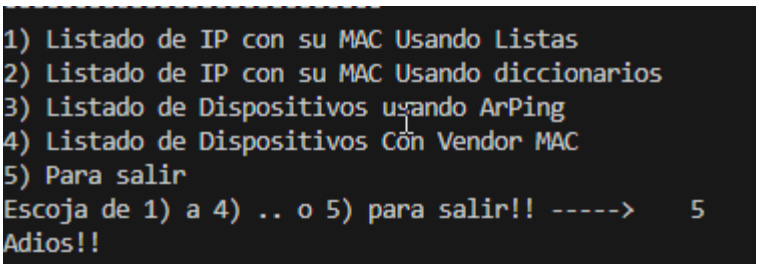



OPCION 4:

LISTADO DE DISPOSITIVOS CON IP Y MAC ADDRESS UTILIZANDO UNA API PARA LISTAR VENDORS



OPCION PARA SALIR




## Conclusión.

Se aprendió mucho del lenguaje python básico

Se utilizo como IDE de programación VISUAL CODE

Y se importaron las librerías

- Scapy
- Requests

La primera para aprender el protocolo ARP

Y la segunda para hacer request a una pagina que tenia el listado de vendors según su mac address.