# Redes de Computadores, 2020
## Tarea 1: Implementación de un OUI Lookup Tool.

Escuela de Ingeniería Informática

Universidad de Valparaíso

Sebastián González Morales

Sebastian.gonzalez@alumnos.uv.cl

## 1 Introducción

Una dirección IP es una dirección empleada para identificar a un dispositivo en una red IP. La dirección se compone de 32 bits binarios, que pueden dividirse en una porción correspondiente a la red y otra correspondiente al host, con la ayuda de una máscara de subred. Los 32 bits binarios se dividen en cuatro octetos. (1 octeto = 8 bits). Cada octeto se convierte a decimal y se separa con un punto. Por esta razón, se dice que una dirección IP se expresa en formato decimal con puntos (por ejemplo, 172.16.81.100). El valor en cada octeto varía de 0 a 255 decimal o 00000000 - 11111111 binario.

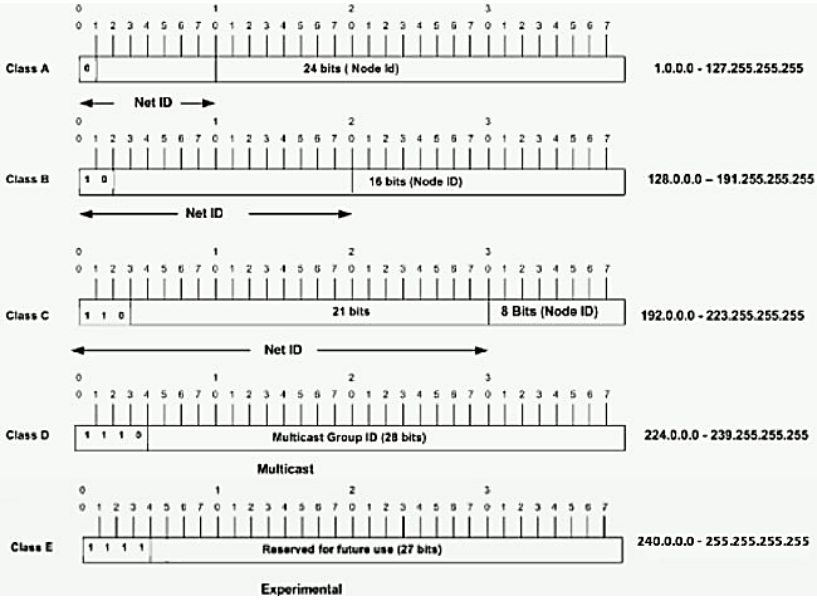
La clase de una dirección IP se puede determinar a partir de los tres bits de gran importancia (los tres bits del extremo izquierdo en el primer octeto). La Figura 1 muestra la importancia de los tres bits de orden superior y el rango de direcciones que pertenecen a cada clase.

En una dirección de Clase A, el primer octeto es la parte de la red, así que el ejemplo de Clase A en la Figura 1 tiene una dirección de red principal de 1.0.0.0 - 127.255.255.255. Los octetos 2,3, y 4 (los 24 bits siguientes) son para que el administrador de la red divida en subredes y hosts como estime conveniente. Las direcciones de Clase A se utilizan para redes que tienen más de 65.536 hosts (en realidad, hasta 16.777.214 hosts).

En una dirección de Clase B, los dos primeros octetos son la parte de la red, así que el ejemplo de Clase B en la Figura 1 tiene una dirección de red principal de 128.0.0.0 - 191.255.255.255. Los octetos 3 y 4 (16 bits) son para subredes locales y hosts. Las direcciones de clase B se utilizan para redes que tienen entre 256 y 65534 hosts.

En una dirección de la Clase C, los tres primeros octetos son la parte de la red. El ejemplo de la clase C en la Figura 1 tiene la dirección de red principal 192.0.0.0 - 223.255.255.255. El octeto 4 (8 bits) es para subredes locales y hosts, perfecto para redes con menos de 254 hosts.[1]

Figura 1




La dirección MAC se toma por defecto de la dirección de hardware de la tarjeta de red. La dirección MAC es un número hexadecimal de 12 dígitos o 48 bits de longitud. Esta dirección la asigna el fabricante del hardware y es única a nivel mundial, por lo que no debe tener direcciones duplicadas en su red (aunque las tarjetas con direcciones duplicadas se han fabricado por errores de producción en el pasado). Por lo general, el problema de las direcciones MAC duplicadas surge porque las personas optan por no usar la dirección de hardware asignada por el proveedor, sino que usan una dirección autoasignada (también llamada dirección administrada localmente). Esta es una técnica utilizada por los piratas informáticos para eludir las restricciones de seguridad basadas en MAC. Esto es más común cuando se utilizan sistemas de tramas principales que se comunican a través de direcciones MAC en lugar de direcciones de protocolo (como direcciones IP). En el último caso, si se reemplaza una computadora o su tarjeta de red debido a una falla de hardware, tendrá que reconfigurar varios sistemas para que funcionen con la nueva dirección MAC, por lo que es mucho más fácil asignar la misma dirección MAC a la nueva tarjeta de red. como la tarjeta fallida. A menos que se encuentre en la pequeña minoría de personas con un sistema como este, o sea un gran hacker, puede ignorar con seguridad la capacidad de administrar su propia dirección MAC[2].

Este documento se estructura de la siguiente forma, en la sección 2 se presentará una descripción del problema. Luego en la sección 3 se explicará la forma de uso del script. En la sección 4 se explicará el diseño y la implementación de la solución. Luego en la sección 5 presentarán pruebas y resultados de

la ejecución del script. En la sección 6 se dará una conclusión sobre el trabajo realizado y finalmente en la sección 7, se mostrarán las referencias utilizadas.

# 2 Descripción del problema

Implementar una herramienta basada en línea de comandos para consultar el fabricante de una tarjeta de red dada su dirección MAC o su IP. La base de datos utilizada para obtener el vendedor de cada dirección mac se encuentra en el archivo https://gitlab.com/wireshark/wireshark/-/raw/master/manuf.

# 3 Modo de uso

El programa se realizó en el lenguaje de programación **pyhton3** y tiene por nombre **OUILookup.py.** Suponiendo que el computador del usuario tiene la ip 192.168.1.30, máscara 255.255.255.0. En las siguientes líneas se puede apreciar el modo de uso en un sistema operativo Linux.

Ejemplo de uso sin parámetros o con la opción `--help`.

```
python3 OUILookup
Use: python3 OUILookup --ip <IP> | --mac <IP> [--help]
--ip : specify the IP of the host to query.
--mac: specify the MAC address to query. P.e. aa:bb:cc:00:00:00.
--help: show this message and quit.
```

Ejemplo de uso con parámetros

Caso ip que pertenezca a su misma red

```
#   python3 OUILookup --ip 192.168.1.5
MAC address : b4:b5:fe:92:ff:c5
Vendor      : Hewlett Packard
```

Caso ip que NO pertenezca a su misma red

```
# python3 OUILookup --ip 192.168.10.5
Error: ip is outside the host network
```

Caso MAC que esté en la base de datos

```
# python3 OUILookup --mac 98:06:3c:92:ff:c5
MAC address : 98:06:3c:92:ff:c5
Vendor      : Samsung Electronics Co.,Ltd
```

Caso MAC que no esté en la base de datos

```
# python3 OUILookup --mac 98:06:3f:92:ff:c5
MAC address : 98:06:3f:92:ff:c5
Vendor      : Not found
```

# 4 Diseño e implementación.

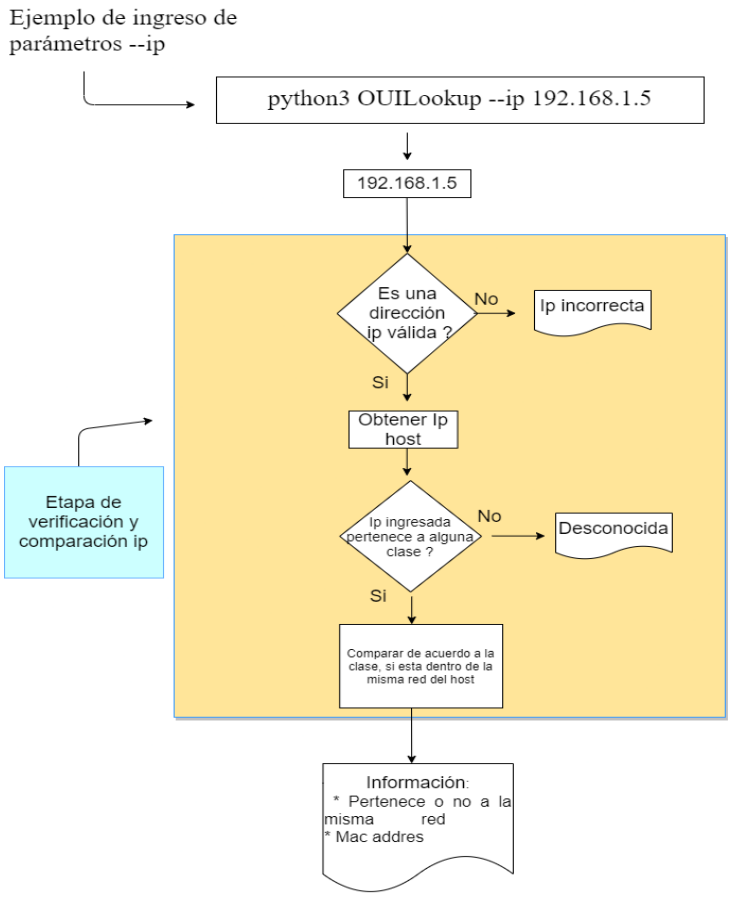
Para realizar el script se utlizaron 4 funciones, estas serán explicadas a continuación:

- **Main():**En esta función se implementa getopt para el ingreso de parámetros del programa, además se verifica que los parámetros y la cantidad de estos sean los correctos.

- **Uso():** Función que se utilizada para mostrar por pantalla la forma de uso del script.

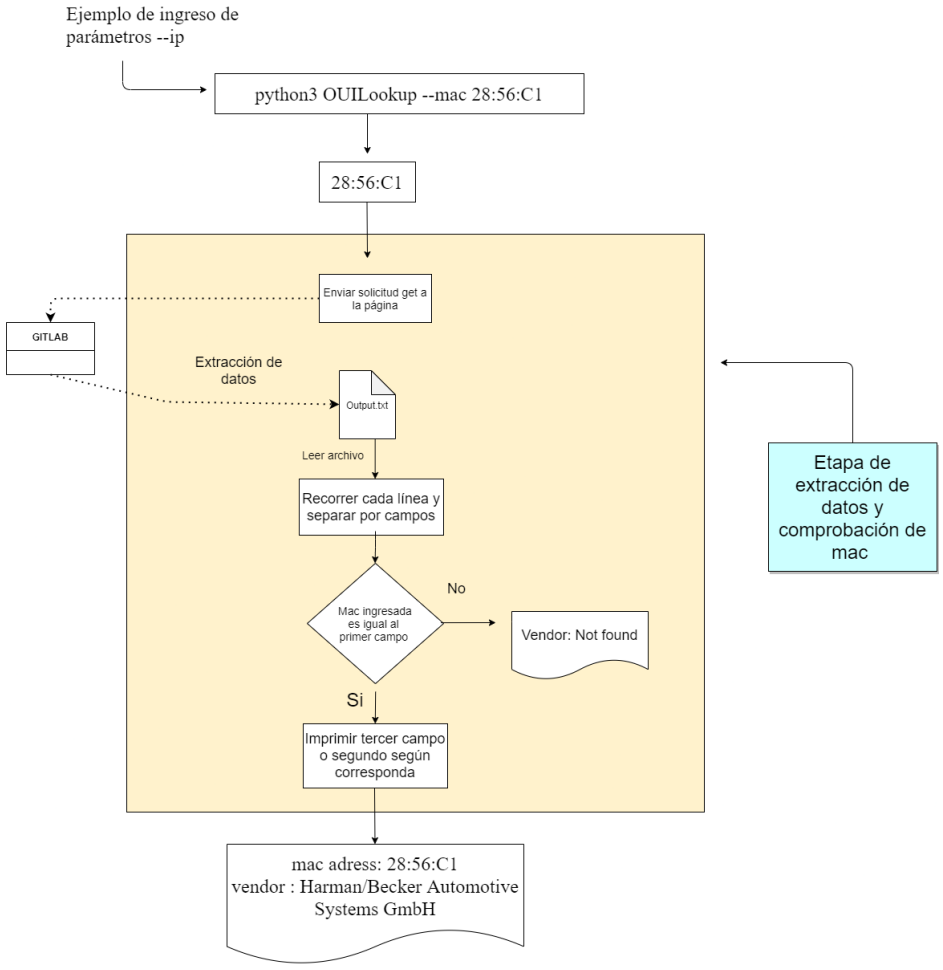
- **Ip():** Lo primero que se realiza en esta función es verificar que al ingresar el parámetro --ip con un valor, este corresponda a una dirección ip, ya sea ipv4 o ivp6, si no corresponde a una de estas llama a la función uso(). Posteriormente, se obtiene la ip del host para luego ser comparada con la ip ingresada y ver si pertenecen a la misma red, para realizar esto, se utilizó la arquitectura class Ful de la que se hablo en la introducción de este trabajo. Luego, se imprime por pantalla la mac adress del host y si la ip ingresada pertenece a la red. Lo anterior se puede apreciar mejor en la figura 2

Figura 2



- **Mac():** Esta función es llamada cuando se coloca el parámetro –mac con el valor de una mac addres. Lo primero que se realiza es enviar una solicitud **GET** a la página que contiene la base de datos con las mac adress y sus fabricantes.. Esta solicitud es el mismo tipo de solicitud que envia un navegador para ver una página web pero la única diferencia es que las solicitudes en realidad no pueden representar el HTML, por lo que en su lugar obtendrá el html sin procesar y la otra información de respuesta. Los datos obtenidos a través de la solicitud GET se redirigen a un archivo de texto llamado output.txt. Luego este archivo es leído línea por línea y si encuentra un valor igual al ingresado, imprimirá el valor del arreglo 3 por pantalla, que corresponde al fabricante de la mac adress.
  Para separar o dividir cada cadena se utilizó la función **Split(),** donde el separador utilizado fue un tabulador (“\t”), cada palabra separada es un elemento del arreglo.Esta función se puede apreciar mejor en la figura 3.

Figura 3



Para la implementación de este script se utilizaron las siguientes librerías de pyhton3

- getopt
- sys
- requests
- re
- ipaddress
- socket
- get_mac_address

# 5 Pruebas de ejecución y resultados.

Las pruebas de ejecución se realizaron en un computador con sistema Linux con la distribución 20.04.

Se le pide al usuario, que antes de ejecutar el script, verifique que tiene instalado Python, de no ser así, ingresar el siguiente comando **sudo apt install python3.** Python utiliza un sistema de gestión y administración de paquetes de sofware, instalarlo con **sudo apt install python3-pip**. También instale el paquete getmac, paquete con el cual se puede obtener dirección MAC de las interfaces de res y los host en la red Local, **pip3 install getmac.**

## 5.1 Pruebas con parámetro ip

En la imagen 1, se puede apreciar una captura de pantalla de la ejecución del programa con el parámetro –ip con la siguiente ip : 223.255.10.1. El programa muestra por pantalla que efectivamente es una IPv4, también muestra la ip del host y dice que la ip ingresada esta fuera de la red del host. Además muestra la mac adress.

Imagen 1

```
sebastian@LAPTOP-PQMOB21:/mnt/c/Redes de computadores$ python3 OUILookup.py --ip 223.255.10.1

223.255.10.1 is a correct IP4 address.

IP of host is: 127.0.1.1

Mac addres  : 00:15:5d:ae:5a:62

Error  : ip is outside the host network
```

En la imagen 2, también se puede apreciar una captura de pantalla, pero a diferencia de la ejecución anterior, ahora se probó otra ip y el programa arrojo que si pertenece a la red del host.

Imagen 2

```
sebastian@LAPTOP-PQMOB21:/mnt/c/Redes de computadores$ python3 OUILookup.py --ip 127.10.10.20

127.10.10.20 is a correct IP4 address.

IP of host is: 127.0.1.1

MAC address  : 00:15:5d:ae:5a:62

Ip is inside the host network
```

En la imagen 3, se puede apreciar que se ingresar cualquier numero y el programa muestra por pantalla que no es una ip, junto con un mensaje del forma de uso.

Imagen 3

```
sebastian@LAPTOP-PQMOB21:/mnt/c/Redes de computadores$ python3 OUILookup.py --ip 1102323434

Ip incorrect

Use: python3 OUILookup.py --ip <IP> | --mac <MAC> [--help]

Parametros:
     --ip: specify the IP of the host to query.
     --mac: specify the MAC address to query. P.e. aa:bb:cc:00:00:00.
     --help: show this message and quit.
```

### 5.2 Pruebas con parámetro mac

En la imagen 4, se puede apreciar una captura de pantalla con el ingreso de parámetros –mac y con una mac addres sacada de la base de datos.

Imagen 4

```
sebastian@LAPTOP-PQMOB21:/mnt/c/Redes de computadores$ python3 OUILookup.py --mac 28:57:BE

MAC address : 28:57:BE
Vendor      : Hangzhou Hikvision Digital Technology Co.,Ltd.
```

En la imagen 5, se puede apreciar que los datos que aparecen en la base de datos de una mac adress son solo dos.

*Imagen 5*

```
28:57:BE        Hangzhou        Hangzhou Hikvision Digital Technology Co.,Ltd.
28:5A:EB        Apple   Apple, Inc.
28:5F:2F        RNware  RNware Co.,Ltd.
28:5F:DB        HuaweiTe        Huawei Technologies Co.,Ltd
28:60:46        LantechC        Lantech Communications Global, Inc.
28:60:94        Capelec
28:63:36        Siemens Siemens AG
28:63:BD        AptivSer        Aptiv Services Us, Llc
28:64:B0        HuaweiDe        Huawei Device Co., Ltd.
```

En la imagen 6, se puede apreciar que el programa fue modificado para casos en donde aparecieran dos datos de lac adress

Imagen 6

```
sebastian@LAPTOP-PQMOB21:/mnt/c/Redes de computadores$ python3 OUILookup.py --mac 28:60:94

MAC address : 28:60:94
Vendor      : Capelec
```

# 7 Conclusión.

Se puede decir que en cierta parte se cumplió con el objetivo requerido, sin embargo, queda al debe el tema de que al ingresar una ip, se puede obtener la mac de esa ip y junto con ello revisar la base de datos para obtener el fabricante.

También decir que con este trabajo se entendieron mejor y se reforzaron los conceptos sobre ip class ful y a la vez mac adress.

# 8 Referencias


[1] IP Addressing and Subnetting for New Users. (2019, 22 julio). Cisco. https://www.cisco.com/c/es_mx/support/docs/ip/routing-information-protocol-rip/13788-3.html

[2] Cisco Networking: MAC Addressing. (2016, 26 marzo). dummies. https://www.dummies.com/programming/networking/cisco/cisco-networking-mac-addressing/