OUILookup: Herramienta de Línea de Comandos para Identificar Fabricantes a Partir de Direcciones MAC

Pablo Medina Valenzuela, **pablo.medina@alunmos.uv.cl**

Cristóbal Javier Soto Carvajal, **cristobal.sotoca@alumnos.uv.cl**

Alonso Venegas Astorga, **alonso.venegas@alumnos.uv.cl**

1. Introducción

En la era digital, las direcciones MAC (Control de Acceso a la Media) juegan un papel esencial en la identificación y comunicación de dispositivos en redes de datos. Cada dispositivo conectado a una red posee una dirección MAC única, que permite identificar al fabricante del hardware, lo cual es relevante tanto para administradores de redes como para investigadores de seguridad. Reconocer a los fabricantes puede ser útil en tareas de administración de redes, auditorías de seguridad y solución de problemas, ya que facilita el rastreo de dispositivos desconocidos y asegura el cumplimiento de las políticas de seguridad de la red.

El objetivo de este proyecto es desarrollar una herramienta llamada "OUILookup", que permita identificar al fabricante de una tarjeta de red a través de su dirección MAC. La idea es que cualquier persona pueda usar esta herramienta desde la línea de comandos y obtener información actualizada sobre los fabricantes, utilizando una API pública.

Con "OUILookup", no solo se simplifica la identificación de dispositivos, sino también la gestión y protección de redes. Conocer a los fabricantes ayuda a rastrear dispositivos y garantizar que cumplan con las políticas de seguridad. Además, la herramienta está diseñada de forma modular y sigue principios de programación funcional, lo que facilita su comprensión y mantenimiento.

En resumen, "OUILookup" busca ser una herramienta útil para quienes necesiten información rápida y confiable sobre dispositivos en la red, con un acceso sencillo y sin complicaciones.

2. Descripción del problema y diseño de la solución

2.1 Descripción del problema

El desafío consiste en identificar a los fabricantes de dispositivos de red basándose en sus direcciones MAC. Cada dirección MAC contiene un código único que permite conocer el fabricante del equipo. Sin embargo, acceder a esta información puede ser complicado, ya que se necesita una base de datos que vincule las direcciones MAC con sus respectivos fabricantes. Para resolver este problema, se requiere una herramienta que permita una consulta rápida y precisa del fabricante de una tarjeta de red a partir de una dirección MAC.

El objetivo de esta herramienta es proporcionar a los administradores de redes y otros usuarios interesados un método sencillo para identificar dispositivos en la red. La herramienta debe ser capaz de gestionar diversas opciones de consulta, que incluyen la verificación individual de una dirección MAC y la revisión de múltiples direcciones a través de la tabla ARP.

2.2 Exigencias y Especificaciones

Para cumplir con su objetivo, la herramienta "OUILookup" debe satisfacer los siguientes requisitos y especificaciones:

Funcionalidad de Línea de Comandos

La herramienta debe funcionar desde la línea de comandos, permitiendo la consulta de fabricantes de tarjetas de red mediante parámetros específicos.

Consulta de Fabricantes

Utilizar una API REST pública para identificar al fabricante asociado a una dirección MAC.

Opciones de Uso

- **Consulta de una MAC específica:** Permitir al usuario ingresar una dirección MAC para obtener el nombre del fabricante.
- **Consulta de la tabla ARP:** Extraer y mostrar una lista de direcciones MAC y sus fabricantes presentes en la tabla ARP del sistema.
- **Ayuda:** Proveer una opción de ayuda que muestre las opciones de uso.

Modularidad y Programación Funcional

El código debe ser modular, fácil de mantener, y seguir principios de programación funcional para facilitar su comprensión y extensibilidad.

Documentación y Diagrama de Flujo

El proyecto debe incluir documentación detallada, un diagrama de flujo que represente el funcionamiento de la herramienta y un diagrama de clases para facilitar la comprensión de su estructura.

2.3 Diseño de la Solución

La herramienta "OUILookup" está diseñada como una aplicación modular que utiliza Python para interactuar con una API pública y obtener información sobre fabricantes de dispositivos. A continuación, se describe el modelo de arquitectura general de la herramienta:

Entrada de Usuario

El usuario interactúa con la herramienta desde la línea de comandos. Se pueden ingresar tres parámetros principales: --mac para consultar una MAC específica, --arp para mostrar todos los fabricantes de las direcciones MAC en la tabla ARP, y --help para ver las opciones de uso.

Solicitudes a la API

Al usar el parámetro --mac, la herramienta realiza una consulta a una API REST pública, que devuelve el fabricante asociado a la dirección MAC solicitada.

Extracción de la Tabla ARP

Con la opción --arp, la herramienta verifica la tabla ARP local para listar todas las direcciones MAC presentes y sus respectivos fabricantes.

Salida de Datos

Los resultados se muestran directamente en la consola. Si se consulta una MAC específica, se presenta el fabricante y el tiempo de respuesta. Si se utiliza la opción --arp, se muestra una lista de direcciones MAC y sus fabricantes.

2.4 Estructura de Clases

Para la implementación de "OUILookup", el diseño incluye las siguientes clases principales:

- **Clase OUILookup:** Administra la interfaz de línea de comandos y organiza la ejecución de las consultas en función de los parámetros proporcionados.
- **Clase MACQuery:** Realiza la consulta de una dirección MAC específica a través de la API.
- **Clase ARPTable:** Gestiona la extracción de la tabla ARP y el mapeo de las direcciones MAC con sus respectivos fabricantes.

Estas clases permiten organizar la lógica de la aplicación de manera clara y modular, separando las responsabilidades principales para facilitar futuras modificaciones y mejoras.

3. Implementación

"OUILookup" es una herramienta desarrollada en Python para su uso desde la línea de comandos, diseñada para facilitar la identificación de fabricantes de dispositivos de red mediante direcciones MAC. A continuación, se detallan los componentes más relevantes del código y su funcionamiento.

3.1. Organización del Código

El programa se organiza en torno a varias funciones que cumplen con roles específicos:

- **Función preguntar_por_mac(mac_address):** Realiza una consulta a la API pública para obtener el fabricante asociado a una dirección MAC proporcionada. Si el fabricante está en la base de datos, devuelve el nombre junto con el tiempo de respuesta.
- **Función preguntar_por_arp():** Extrae y muestra las direcciones MAC de la tabla ARP del sistema y sus respectivos fabricantes.
- **Función tabla_rubrica():** Muestra un mensaje de ayuda que explica cómo usar la herramienta.
- **Función main(argv):** Es la función principal que gestiona el flujo del programa. Lee los argumentos de línea de comandos y redirige a las funciones correspondientes según las opciones ingresadas (--help, --mac, --arp).

3.2. Aplicación del Diagrama de Flujo

El **Diagrama de Flujo** a continuación ilustra el proceso de toma de decisiones dentro de la función principal main(argv). Este diagrama muestra cómo el programa selecciona la ruta correcta de acuerdo con la opción de entrada:

- **Consulta de Asistencia (--help):** Invoca la función tabla_rubrica para mostrar las instrucciones de uso.
- **Consulta de una Dirección MAC (--mac):** Llama a la función preguntar_por_mac para obtener el fabricante y presenta el resultado.
- **Acceso a la Tabla ARP (--arp):** Activa la bandera de la tabla ARP y llama a preguntar_por_arp para mostrar la lista de direcciones MAC y sus fabricantes.

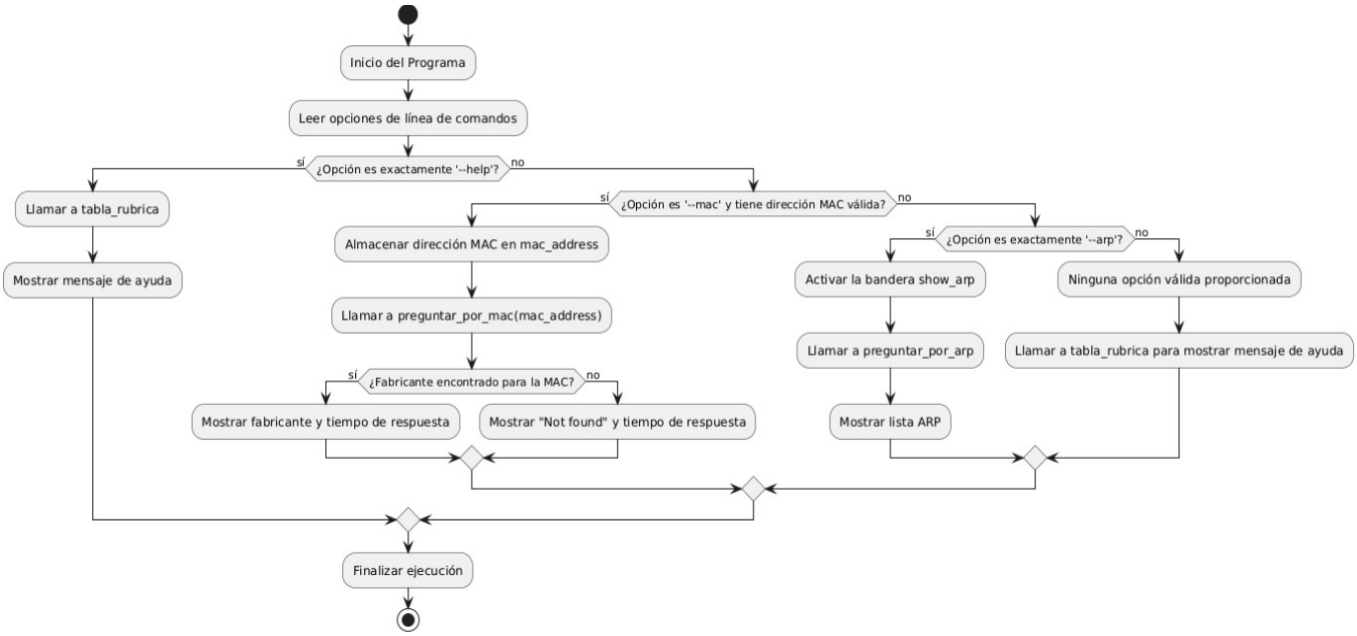

Figura 1. El diagrama muestra el flujo de operaciones de la herramienta "OUILookup". El programa comienza leyendo las opciones ingresadas por el usuario y sigue diferentes rutas según la entrada: --help para mostrar ayuda, --mac para consultar un fabricante específico, o --arp para listar la tabla ARP. Si no se proporciona una opción válida, se muestra el mensaje de ayuda.

3.3. Problemas y Soluciones

Un desafío importante fue asegurar que el programa gestionara correctamente las entradas inválidas y las excepciones en las consultas a la API. Se implementó un manejo de errores que captura posibles problemas de red o fallos en las solicitudes a la API, proporcionando mensajes claros al usuario. Además, el programa fue diseñado de manera modular y flexible, facilitando el mantenimiento y futuras expansiones.

4. Pruebas

Para asegurar el correcto funcionamiento de la herramienta "OUILookup", se llevaron a cabo varias pruebas utilizando los tres parámetros principales: --mac, --arp, y --help. A continuación, se detallan los casos de prueba realizados, sus resultados, y cómo se verificó la efectividad del código.

4.1. Prueba de Direccion MAC (--mac)

```
PS C:\Users\xunxi\OneDrive\Escritorio> python OUILookup.py --mac 98:06:3c:92:ff:c5
MAC address : 98:06:3c:92:ff:c5
Fabricante  : Samsung Electronics Co.,Ltd
Tiempo de respuesta: 631 ms
```

Figura 2. En este caso, se ejecutó el comando con una dirección MAC específica para identificar al fabricante asociado.

Resultado: El software devolvió el fabricante correspondiente, "Samsung Electronics", junto con el tiempo de respuesta, lo que confirma que la consulta a la API fue exitosa y precisa.

4.2. Prueba de Acceso a la Tabla ARP (--arp)

```
PS C:\Users\xunxi\OneDrive\Escritorio> python OUILookup.py --arp
MAC/Vendor:
00:01:97:bb:bb:bb / Cisco
b4:b5:fe:92:ff:c5 / Hewlett Packard
00:E0:64:aa:aa:aa / Samsung
AC:F7:F3:aa:aa:aa / Xiaomi
```

Figura 3. Se probó el comando para listar los fabricantes de las direcciones MAC presentes en la tabla ARP del sistema.

Resultado: El software mostró una lista de direcciones MAC y sus respectivos fabricantes, incluyendo "Cisco", "Hewlett Packard", "Samsung" y "Xiaomi". Esto verificó que la herramienta podía acceder y mostrar adecuadamente los datos de la tabla ARP.

4.3. Prueba de Ayuda (--help)

```
PS C:\Users\xunxi\OneDrive\Escritorio> python OUILookup.py --help
Uso: OUILookup.py --mac <mac> | --arp | [--help]
  --mac: MAC a consultar. P.e. aa:bb:cc:00:00:00.
  --arp: muestra los fabricantes de los host
         disponibles en la tabla arp.
  --help: muestra este mensaje y termina.
```

Figura 4. Ejecucion y funcionamiento del commando help.

Resultado: El software mostró correctamente un mensaje de ayuda con las opciones disponibles (--mac, --arp, y --help), lo que asegura que el usuario puede acceder a instrucciones en cualquier momento.

4.4. Conclusiones de las Pruebas

Cada parámetro fue evaluado de manera independiente, y en todas las pruebas el programa cumplió con las expectativas, mostrando la información solicitada o el mensaje de ayuda de manera precisa. Se comprobó la funcionalidad con diversas entradas para garantizar la estabilidad y precisión de las respuestas, tanto en la consulta de fabricantes específicos como en la extracción de datos de la tabla ARP.

5. Mac aleatorias

El uso de direcciones MAC aleatorias es una técnica que se emplea para aumentar la privacidad de los usuarios cuando se conectan a redes Wi-Fi. Esta función permite que los dispositivos generen direcciones MAC temporales y aleatorias en lugar de usar la dirección única y fija que les asigna el hardware de red. De esta manera, los dispositivos pueden evitar ser fácilmente rastreados por redes y observadores, ya que cada vez que se conectan a una red nueva —o incluso a la misma red en diferentes momentos— muestran una identidad digital temporal diferente.

La aleatorización de direcciones MAC comenzó a implementarse ampliamente en dispositivos móviles en 2014, y hoy es una función estándar en sistemas operativos como Android, iOS, y Windows. Por ejemplo, Apple permite que los iPhones generen una dirección MAC aleatoria para cada red Wi-Fi a la que se conectan, lo cual ayuda a proteger la identidad del usuario y reduce el riesgo de ser rastreado en redes públicas. Sin embargo, este proceso no es completamente automático en todas las plataformas. En algunos casos, como en macOS, los usuarios deben activar esta función manualmente.

Si bien la aleatorización de MAC ofrece ventajas significativas, como la reducción del riesgo de monitoreo, también presenta desafíos, especialmente en entornos corporativos. En estos contextos, donde la administración de redes suele depender de las direcciones MAC para controlar el acceso y solucionar problemas, la aleatorización puede complicar la

gestión de la red. Por esta razón, algunas empresas optan por restringir o gestionar esta función en sus redes internas para mantener un control más eficiente.

Bibliografía:

[1] https://cloud.wikis.utexas.edu/wiki/spaces/EndpointManagement/pages/57739479/MAC+Address+Randomization+How+it+works+and+What+IT+needs+to+know

[2] https://www.commscope.com/blog/2020/so-whats-the-big-deal-about-mac-randomization/

[3]https://www.kandji.io/definitions/mac-address-randomization/#:~:text=It%20masks%20the%20identity%20of,to%20track%20activity%20across%20others.

6. Discusión y conclusiones

6.1. Resumen de Resultados

El programa "OUILookup" alcanzó los objetivos propuestos, facilitando la identificación de fabricantes de dispositivos de red a partir de direcciones MAC. Las pruebas realizadas confirmaron la precisión de las consultas a la API y la capacidad de obtener y mostrar información de la tabla ARP. Además, el programa demostró ser robusto y estable al gestionar correctamente las opciones de uso y manejar eventuales fallos.

6.2. Reflexiones y Aprendizajes

El desarrollo de "OUILookup" permitió aplicar y consolidar conocimientos en programación de línea de comandos, integración con APIs y manejo de errores. Un aprendizaje clave fue la importancia de gestionar adecuadamente los posibles fallos de red para garantizar una experiencia de usuario consistente. Sin embargo, un aspecto pendiente fue la gestión de direcciones MAC aleatorias, que podría mejorar la precisión en redes donde se prioriza la privacidad.

6.3. Mejoras Potenciales

Aunque la herramienta cumple sus objetivos, existen áreas con potencial de mejora:

- **Optimización del Tiempo de Respuesta:** Investigar métodos para reducir los tiempos de consulta a la API, mejorando así la eficiencia.
- **Soporte para MAC Aleatorias:** Ampliar la capacidad de la herramienta para reconocer y gestionar direcciones aleatorias, optimizando su uso en entornos de alta privacidad.
- **Interfaz Gráfica:** La incorporación de una interfaz visual podría facilitar el uso para usuarios no técnicos, haciendo la herramienta más accesible.

- **Registro de Consultas:** Añadir una opción para guardar y consultar el historial de búsquedas podría ser útil para administradores de redes.

En conclusión, "OUILookup" es una herramienta eficaz y práctica para la identificación de fabricantes de dispositivos de red. Con algunas mejoras, podría ajustarse aún mejor a diversos contextos y necesidades de los usuarios.