Análisis de tráfico de redes locales usando Teoría de la Información

Alexis Balbachan Manuel Costa Mathias Gatti

Resumen —

Index Terms —**entropía, Teoría de la informacin, ARP, LAN, unicast, broadcast, sniffing**

I. Introducción

Iniciamos este trabajo con el objetivo de aprender sobre el protocolo ARP y más en general las redes de Internet y sus algoritmos de intercambio de paquetes.

A lo largo de este informe describiremos ciertos análisis que tendrán como objetivo el modelado de emisores de información y la posterior detección de símbolos destacados. A partir de esta metodología creemos que podremos identificar dispositivos claves en la red como por ejemplo el gateway. Nuestra hipótesis es que este tendrá destacará en el intercambio de paquetes who-has siendo de los que mas reciba y envíe.

II. Métodos

Herramientas

Para la captura de tráfico se utilizó el módulo de manipulación de paquetes *Scapy* para python, el cual provee una interfaz sencilla para nuestros requerimientos puntuales. *Scapy* permite la captura y posterior guardado de paquetes en una red, para luego ser filtrados, inspeccionados o manipulados con facilidad. Además, para incrementar la cantidad de paquetes vistos por un host, se activó el modo promiscuo o modo monitor en sus respectivas interfaces de red.

Modelo de las fuentes

Fuente S1

Dado el tráfico de capa 2 obtenido en cada captura, se modeló una fuente de memoria nula S1 = $\{s_1, s_2, s_3, ..., s_n\}$ donde cada s_i está formado por una tupla ¡broadcast—unicast, protocolo capa 3¿.

Fuente S2

Igualmente que S1, se modeló la fuente de memoria nula S2 con el objetivo utilizando sólo las direcciones IP dentro de paquetes de protocolo ARP con el objetivo de poder distinguir los hosts de cada red. En este caso se consideraron diversas opciones para el modelado de la fuente, donde cada s_i representaba las direcciones IP de los hosts, aunque su contabilización se regía por si la dirección aparecía en los campos:

- Fuente o Destino
- who-has Fuente
- who-has Destino
- is-at Fuente
- is-at Destino

Capturas

Se hicieron 3 capturas en redes diferentes de 10000 paquetes cada una:

- Red hogareña mediana, con aproximadamente 10 usuarios, se utilizó una interfaz ethernet.
- Red pública grande, en este caso se capturó mediante una interfaz wifi el tráfico del laboratorio de informática de la universidad.
- Red pública grande, también mediante la interfaz wifi, se capturó el tráfico en un Starbucks.

III. Resultados y análisis

Red hogareña

Resultados fuente S1

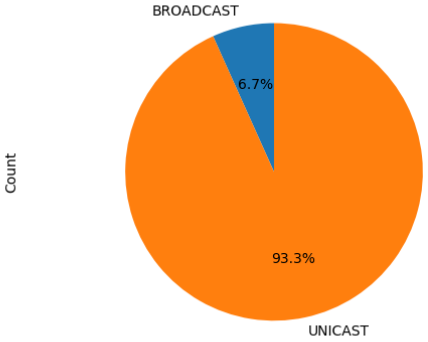

Figura 1: Proporción de paquetes unicast/broadcast en la captura

A. Balbachan e-mail: alexisbalbachan@gmail.com
M. Costa, e-mail: manucos94@gmail.com
M. Gatti, e-mail: mathigatti@gmail.com

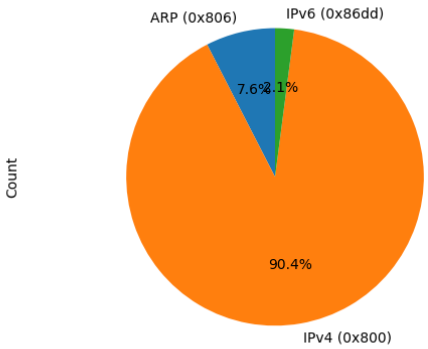

Figura 2: Proporción de protocolos en la captura

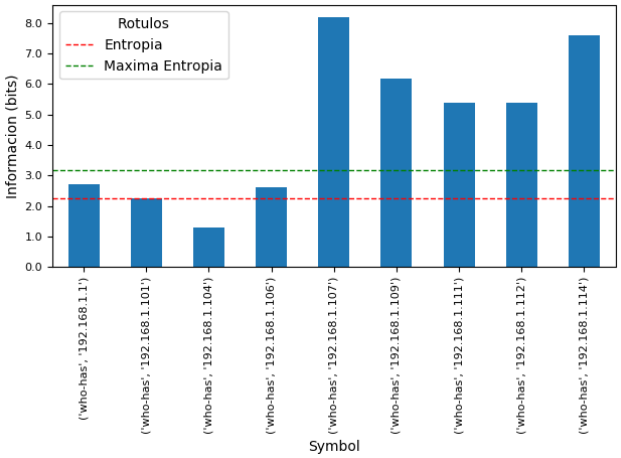

Figura 4: Información de los símbolos de la fuente S2, notando la entropía de la fuente, y la máxima entropía posible si la fuente fuera equiprobable.

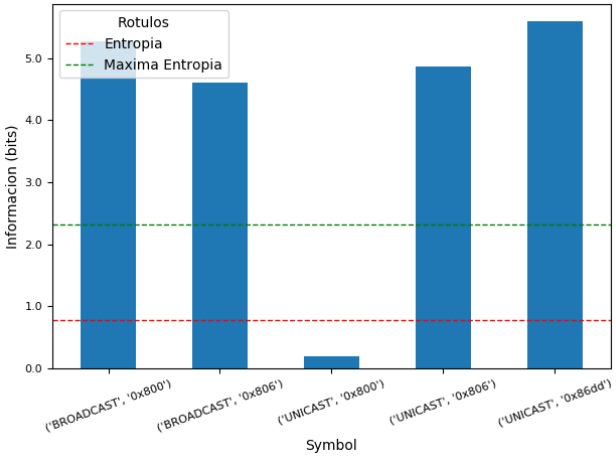

Figura 3: Información de los símbolos de la fuente S1, notando la entropía de la fuente, y la máxima entropía posible si la fuente fuera equiprobable.

Resultados fuente S2

A partir de los paquetes que se intercambian en distintas redes vemos los grafos subyacentes a las mismas. En estos cada vertice representa una IP local y cada arista va del origen al destino de un paquete who-has del protocolo ARP.

En este grafo los dos nodos con mayor grado son 192.168.1.1 con grado 7 y 192.168.1.112

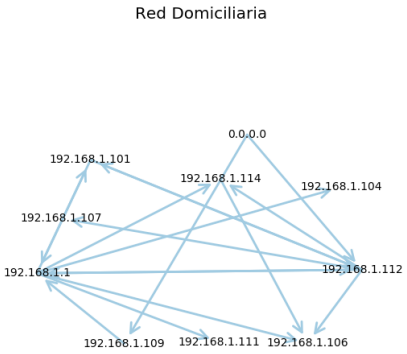

Figura 5: Grafo resultante de la red ethernet de una red domiciliaria durante la noche de un día de semana.

Este grafo tiene solo dos nodos de los cuales el único que recibe paquetes es el nodo 172.19.96.1

Red laboratorios

Resultados fuente S1

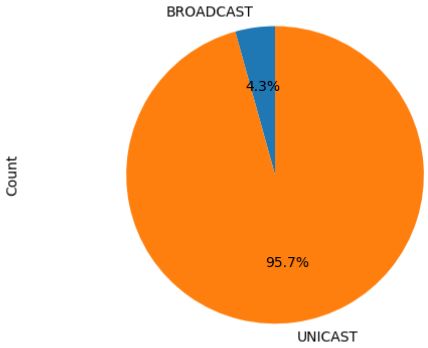

Figura 6: Proporción de paquetes unicast/broadcast en la captura

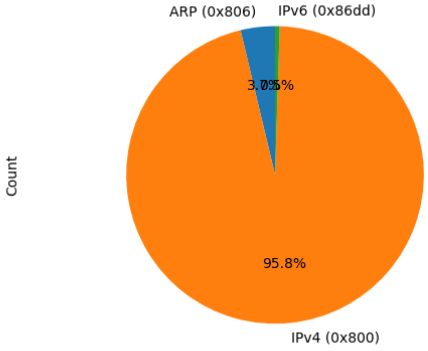

Figura 7: Proporción de protocolos en la captura

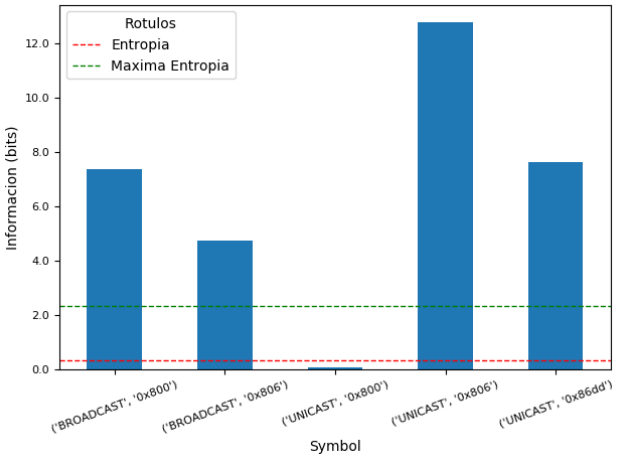

Figura 8: Información de los símbolos de la fuente S1, notando la entropía de la fuente, y la máxima entropía posible si la fuente fuera equiprobable.

Resultados fuente S2

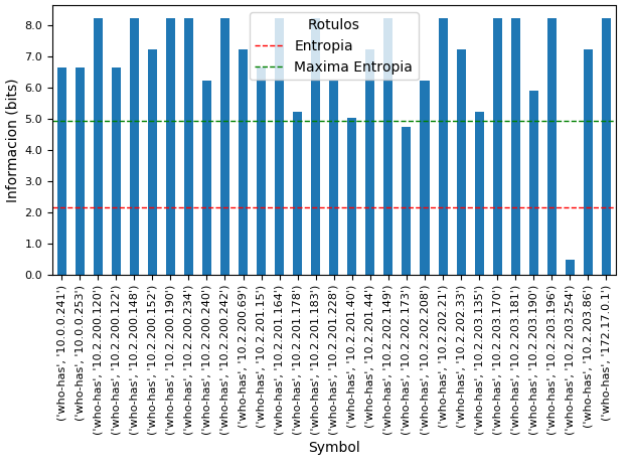

Figura 9: Información de los símbolos de la fuente S2, notando la entropía de la fuente, y la máxima entropía posible si la fuente fuera equiprobable.

Este grafo es mucho mas grande que los anteriores y cuenta con un nodo de máximo grado el cual es el 10.2.203.254.

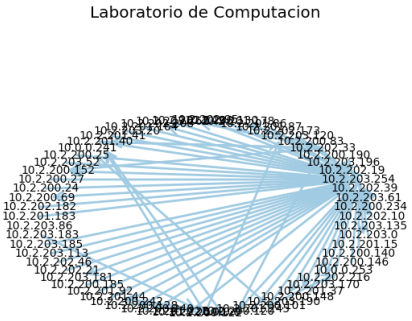

Figura 10: Grafo resultante de la red wifi del laboratorio de computación de la facultad a las 18 PM de un miércoles.

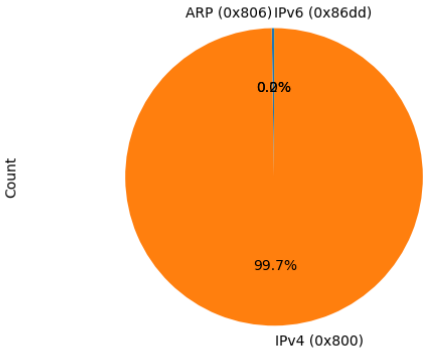

Figura 12: Proporción de protocolos en la captura

Red Starbucks

Resultados fuente S1

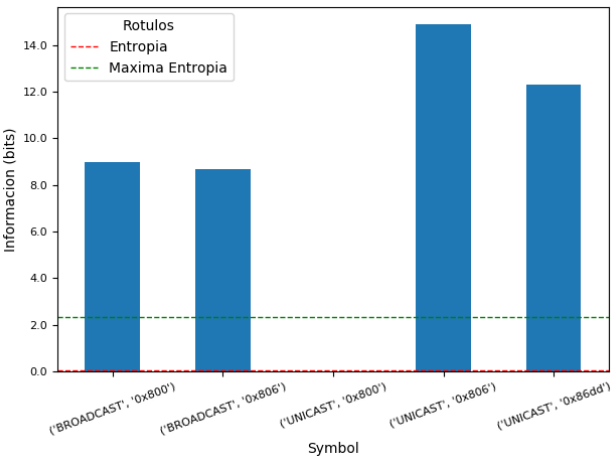

Figura 13: Información de los símbolos de la fuente S1, notando la entropía de la fuente, y la máxima entropía posible si la fuente fuera equiprobable.

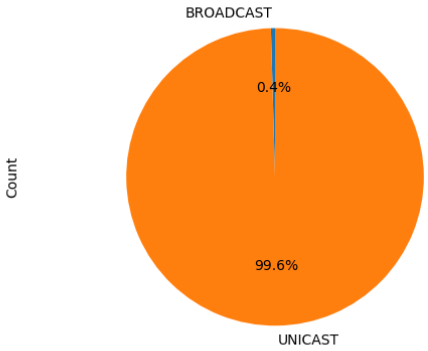

Figura 11: Proporción de paquetes unicast/broadcast en la captura

Resultados fuente S2

Este grafo tiene solo dos nodos de los cuales el unico que recibe paquetes es el nodo 172.19.96.1

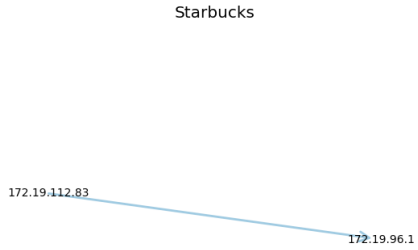

Figura 14: Grafo resultante de la red wifi de una red pública en un starbucks durante la tarde de un día de semana.

IV. Discusión

Como resultado final pudimos identificar de distintas maneras nodos destacados, por ejemplo a partir del grafo subyacente que armamos pudimos identificar en todos los casos al gateway a partir del nodo de mayor grado. A continuación describimos brevemente cada caso analizado por separado.

.1 Red Domiciliaria

En la red domiciliaria se pudo ver en el grafo resultante como destacaban dos nodos. Uno de ellos, el de mayor grado, era el gateway, el otro creemos que fue la computadora que tomó las mediciones ya que estaba accediendo a multiples sitios de internet lo cual provoco un gran intercambio de paquetes.

.2 Laboratorio de Computación

Este es el grafo mas grande y en el cual se vuelve aún mas claro el patrón que veniamos viendo, el nodo 10.2.203.254 resalta completamente de los demás y concuerda perfectamente con nuestra hipotesis de que el gateway es el que mas paquetes intercambia en este protocolo, lo cual lo vuelve un nodo destacado.

.3 Starbucks

Quizas por una mala configuración de la red o por la poca clientela que había en este local en el horario en que se tomaron las mediciones (7:10 AM) es que este grafo resultó ser tan pobre, de todas maneras se pueden observar perfectamente los dos nodos que uno esperaría ver como minimo. El gateway y la computadora que tomo las mediciones.

«“¡Updated upstream

»”’.4 Laboratorio de Computación

»”’Este es el grafo mas grande y en el cual se vuelve aún mas claro el patrón que veniamos viendo, el nodo 10.2.203.254 resalta completamente de los demás y concuerda perfectamente con nuestra hipótesis de que el gateway es el que mas paquetes intercambia en este protocolo, lo cual lo vuelve un nodo destacado. ======= ””»¿Stashed changes