Teoría de las Comunicaciones

Segundo cuatrimestre 2017

Departamento de Computación
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Grupo 6

TP1

Integrante	LU	Correo electrónico
Alejandro Ferrante	371/09	matapalabras@hotmail.com
Gonzalo Guillamon	97/12	gonzaguillamon@gmail.com
Malena Ivnisky	421/12	malenaivnisky@gmail.com

Índice

1. Resumen

En este trabajo práctico realizamos mediciones sobre tres redes diferentes, dos domésticas y una pública. Las analizamos en función de dos modelos de fuentes, y vimos las redes de mensajes ARP subyacentes, que eran muy simples en el caso de las redes domésticas y muy complicada en el caso de la red pública. En general vimos los protocolos que esperábamos ver y uno que no conocíamos. Vimos muchas similitudes entre las dos redes domésticas.

2. Introducción

El objetivo de este trabajo práctico es analizar distintas capturas de red usando las herramientas vistas en la materia.

3. Justificación de la elección de la fuente S2

El objetivo de la fuente S2 es poder distinguir a los hosts de cada red, usando las IP dentro de los paquetes ARP capturados. Propusimos un modelo en el cual los símbolos son las IPs de los emisores de paquetes ARP del tipo who-has. Esto nos permite distinguir entre hosts comunes y routers, ya que esperamos que los routers envíen muchos más requests de ARP que el resto de los dispositivos conectados.

En este caso un host distinguido sería uno que envíe muchos requests de ARP.

4. Experimento 1: Red de Starbucks

4.1. Descripción del contexto

El experimento fue realizado en una red de FibertelZone, por medio de una conexión Wi-Fi en un local de Starbucks de Corrientes y Malabia. Dentro de la red se encuentran conectadas aproximadamente 10 notebooks y muchos celulares, además del router. La fecha de captura es Lunes 9 de Octubre de 2017.

4.2. Descripción de la captura

Capturamos 12000 paquetes. En la figura 1 se muestra la distribución de los protocolos en la red. Observamos que la mayoría de los paquetes son de tipo IPv4, otros son de tipo `0x86dd` (IPv6) y la minoría son de ARP.

Los paquetes de tipo IPv4 e IPv6 usan distintas versiones del protocolo IP. Los paquetes de tipo ARP son los usados por los hosts de una red para obtener direcciones MAC de otros dispositivos, a partir de su IP.

Esto es consistente, ya que la mayoría de los dispositivos usan IPv4/IPv6 para conectarse a Internet, y el porcentaje de paquetes ARP es considerable al haber muchos dispositivos conectados al mismo tiempo.

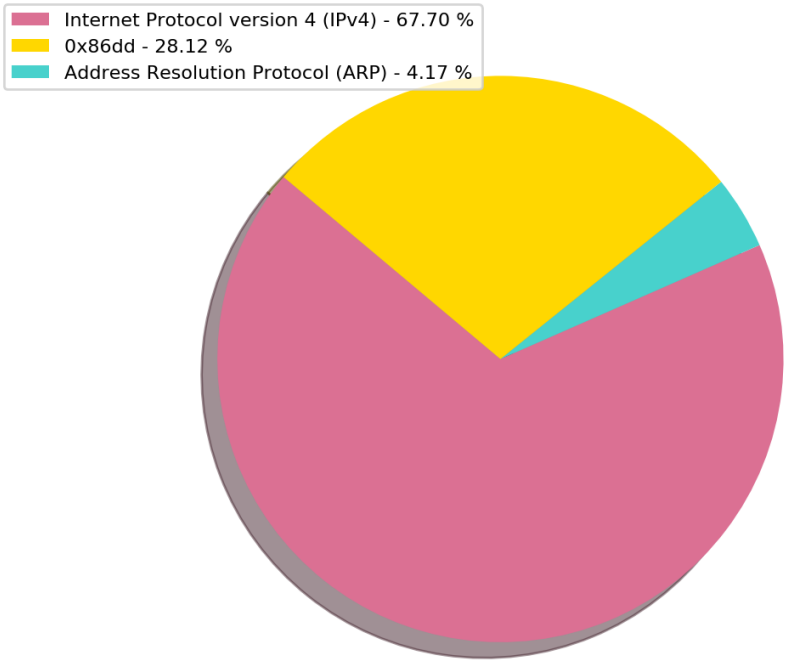

Figura 1: Gráfico que muestra la distribución de protocolos en la red.

En la figura 2 podemos ver el porcentaje de paquetes broadcast comparado con el total de paquetes. Vemos que esto representa un 16 % del total. En la figura 3 vemos que los protocolos que aparecen en los paquetes de broadcast son ARP e IPv4. En cuanto a ARP, estos paquetes son los del tipo who-is, que mediante broadcast llegan al nodo cuya IP busca el emisor.

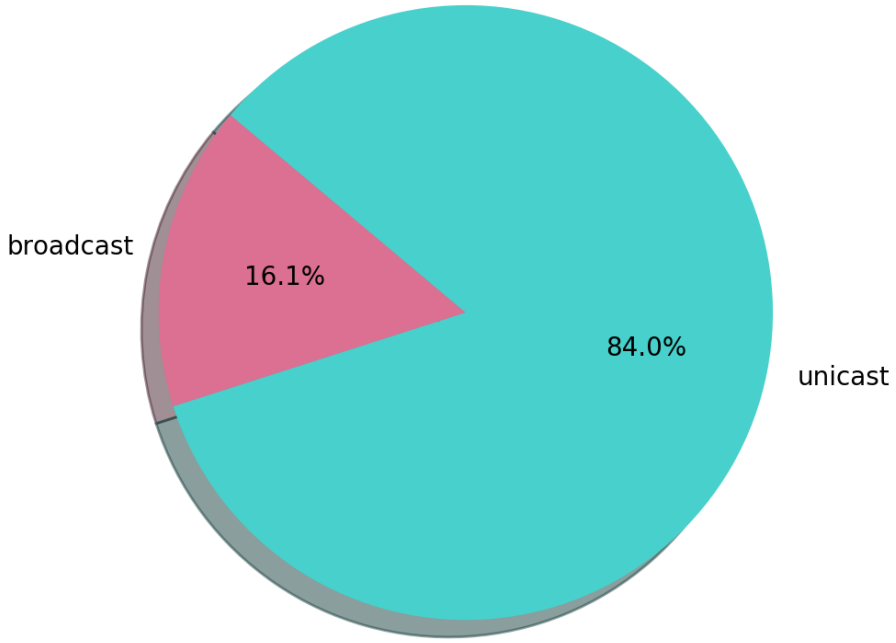

Figura 2: Gráfico que muestra los porcentajes de tráfico broadcast y unicast.

4.3. Análisis de la captura

Realizamos el modelado de la fuente S_1 según el enunciado. En la figura 3 se encuentra el gráfico de la información de cada símbolo. Cuanta más información tenga un símbolo, quiere decir que es menos probable que aparezca. En esta red particular el símbolo con más información es representado por los paquetes unicast de tipo ARP. Estos paquetes

son los is-at, las respuestas a los who-has. Tiene sentido ya que mientras que el request de ARP se hace mediante broadcast (o sea, mandando muchos paquetes), el reply es unicast (menos paquetes).

Además vemos que la entropía muestral es más de la mitad de la entropía máxima, esto es así porque la información de los distintos símbolos es comparable. El símbolo con más información (ARP, unicast) tiene aproximadamente 10 veces la información del menor (IPv4, unicast). La entropía máxima se alcanzaría si la información de todos los símbolos fuese la misma.

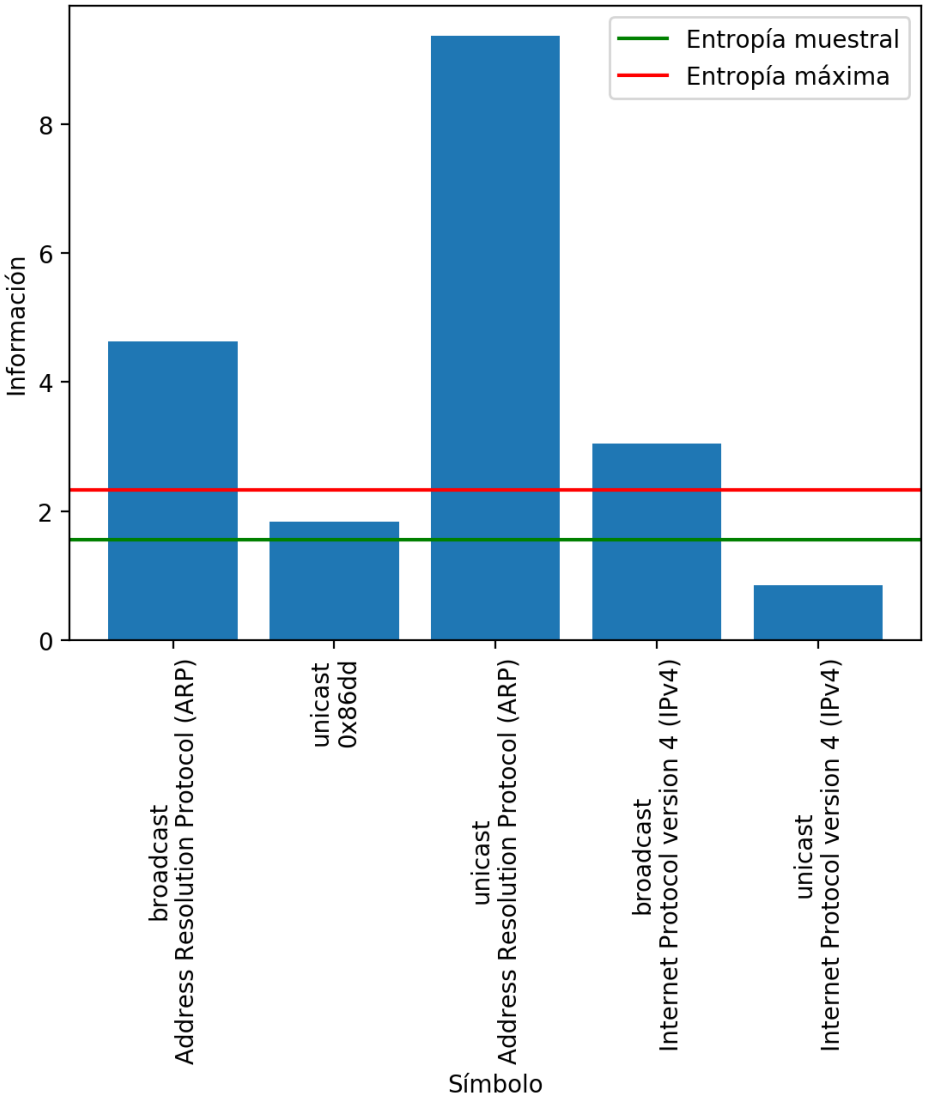

Figura 3: Gráfico de la información de los símbolos de la fuente S_1 observados en esta red. Se muestra la entropía muestral de S_1 y su entropía máxima.

El análisis usando el modelado de la fuente S_2 (explicado anteriormente) se puede ver en la figura 4. En este caso vemos que los símbolos de la fuente podrían dividirse en 2 o 3 grupos de acuerdo a su información. Se observan algunos puntos distinguidos, en particular las 8 IPs con información menor a la entropía de S_2. Estas son las IPs que más requests de ARP hicieron.

La entropía muestral es aproximadamente $\frac{4}{5}$ de la máxima. Es alta ya que hay muchos símbolos con valores parecidos de información; la máxima se alcanzaría con equiprobabilidad.

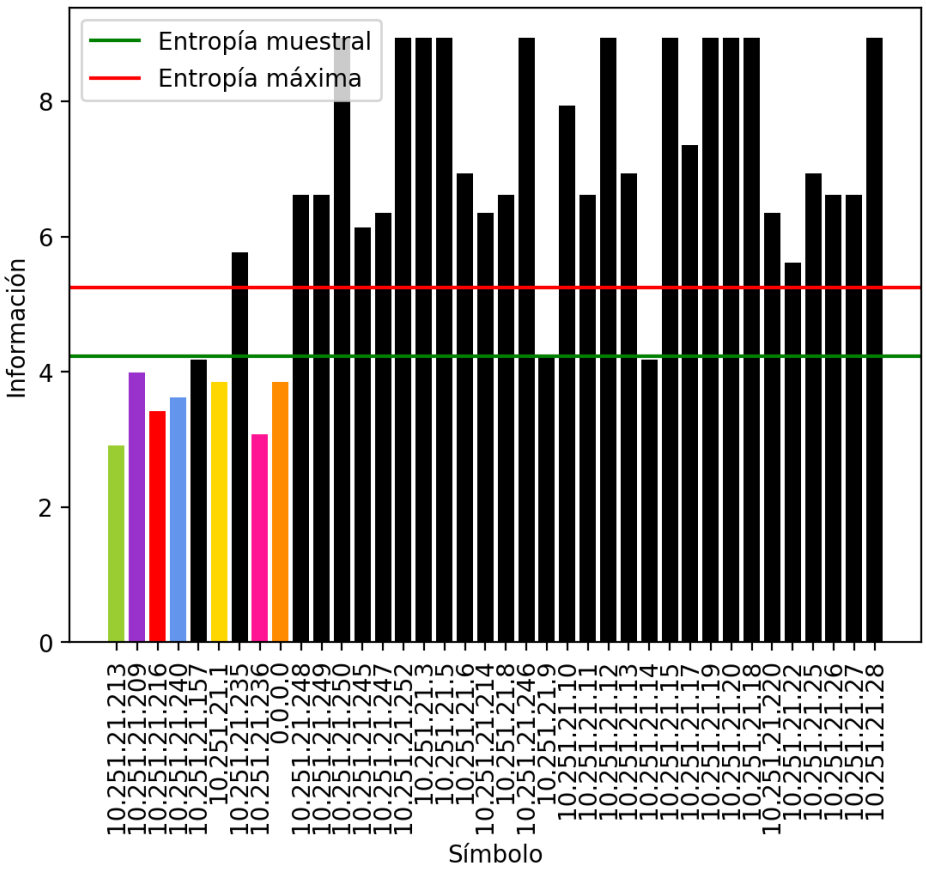

Figura 4: Gráfico de la información de los símbolos de la fuente S_2 observados en esta red. Se muestra la entropía muestral de S_2 y su entropía máxima.

Por último graficamos la red subyacente de mensajes ARP, en la figura 5. Cada nodo del grafo representa una IP interviniente en al menos un mensaje ARP de la red, y cada eje orientado representa que la primera IP envió al menos un mensaje a la segunda. No estamos distinguiendo entre paquetes de tipo who-has o is-at. Podemos ver que el nodo central se comunica separadamente con muchos otros nodos, por lo que creemos que es el router del Stabucks.

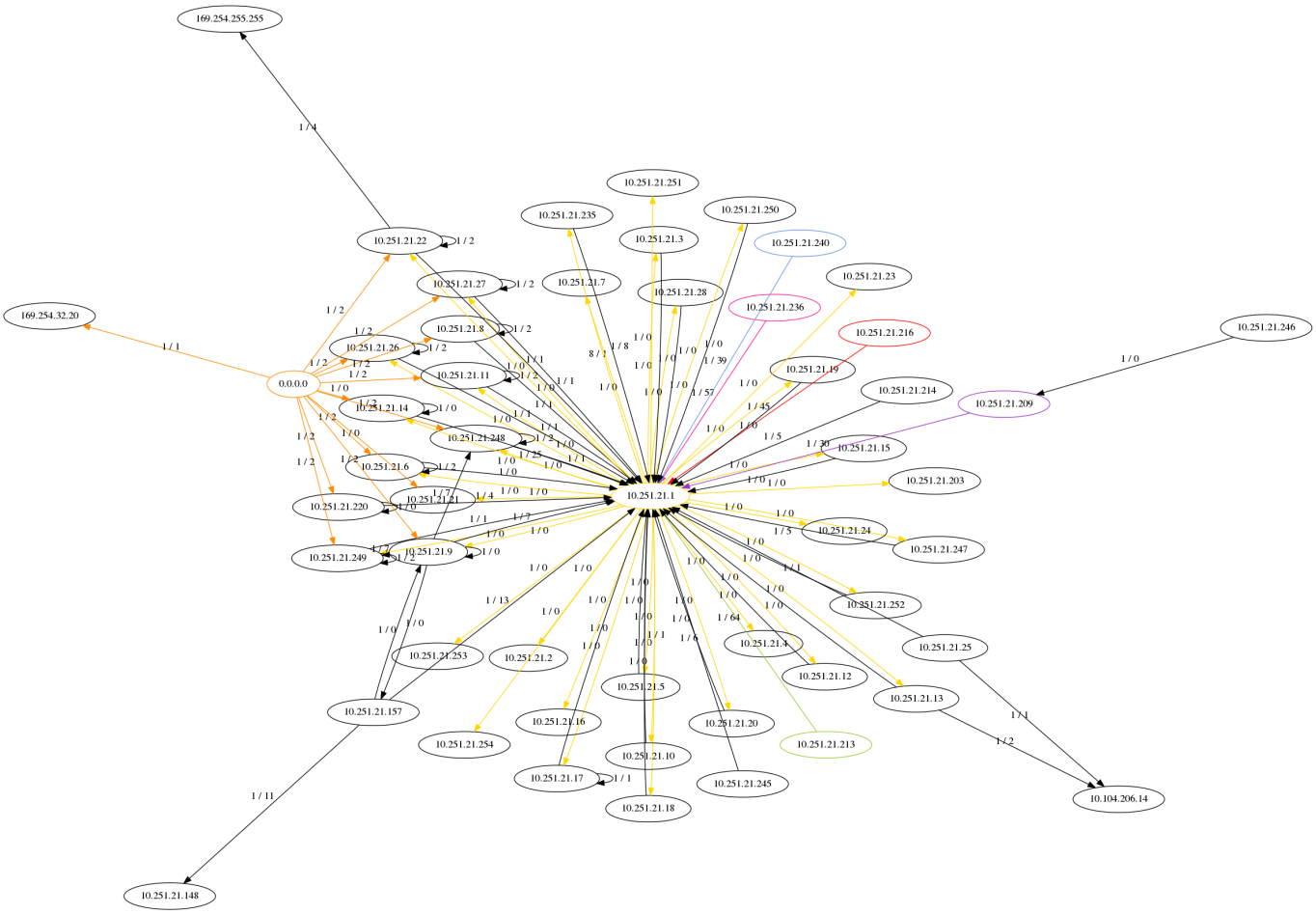

Figura 5: Grafo de la red de mensajes ARP subyacente. Los nodos son las IPs observadas y los ejes son los mensajes ARP. En rojo se marcan los nodos distinguidos (información por debajo de la entropía) y sus mensajes salientes. Cada arista tiene anotada la cantidad de requests/replies ARP.

5. Experimento 2: Red hogareña

5.1. Descripción del contexto

El experimento fue realizado en una red doméstica, por medio de una conexión Wi-Fi de Fibertel. Al momento de tomar las mediciones estaban conectados a la red una laptop, una smart TV, un celular y una tablet, entre otras cosas. La fecha de la captura fue Sábado 7 de Octubre de 2017. El celular estaba siendo usado para controlar el programa VLC por remoto.

5.2. Descripción de la captura

Capturamos 10000 paquetes. En la figura 6 se muestra la distribución de protocolos dentro de la captura. Observamos que hay paquetes de tipo IPv4, `0x86dd` (IPv6), ARP y también Fast Roaming Internet Request. Este último es un protocolo que permite la comunicación continua con dispositivos en movimiento.

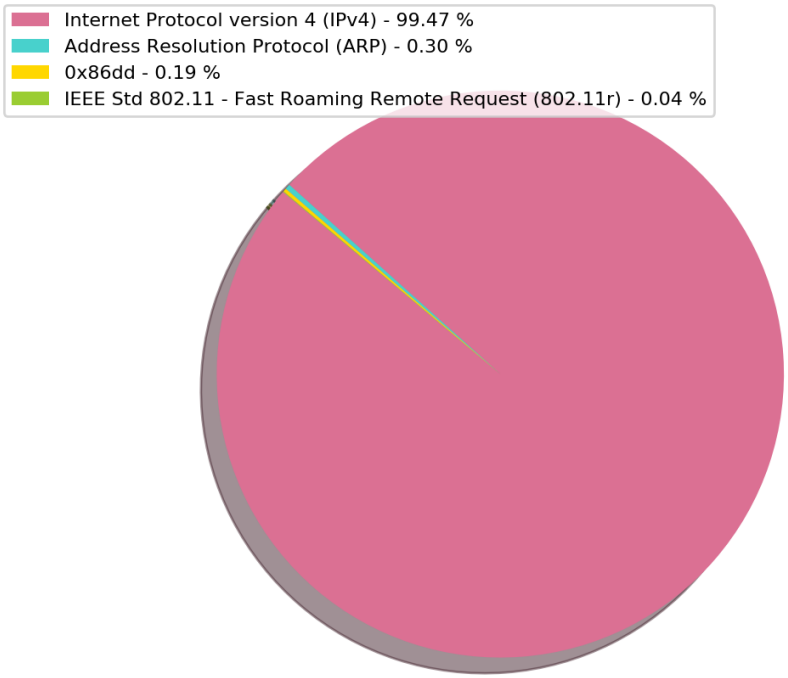

Figura 6: Gráfico que muestra la distribución de protocolos en la red.

En la figura 7 podemos ver el porcentaje de paquetes broadcast comparado con el total de paquetes. Vemos que esto representa un 1,8 % del total. En la figura 8 vemos que los protocolos que aparecen en los paquetes de broadcast son ARP e IPv4. El porcentaje de broadcast es mucho menor al de la primer red porque hay menos dispositivos en uso.

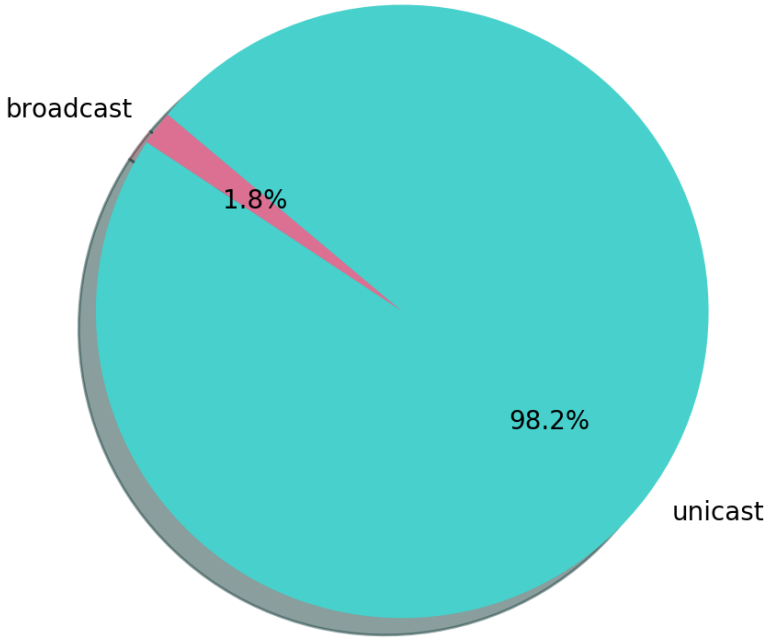

Figura 7: Gráfico que muestra los porcentajes de tráfico broadcast y unicast.

5.3. Análisis de la captura

En la figura 8 se encuentra la información de cada símbolo de la fuente S_1 para esta red. Observamos que hay un símbolo cuya información es muy baja en comparación con la de los demás (IPv4, unicast); y esto hace que la entropía muestral sea mucho menor a la máxima.

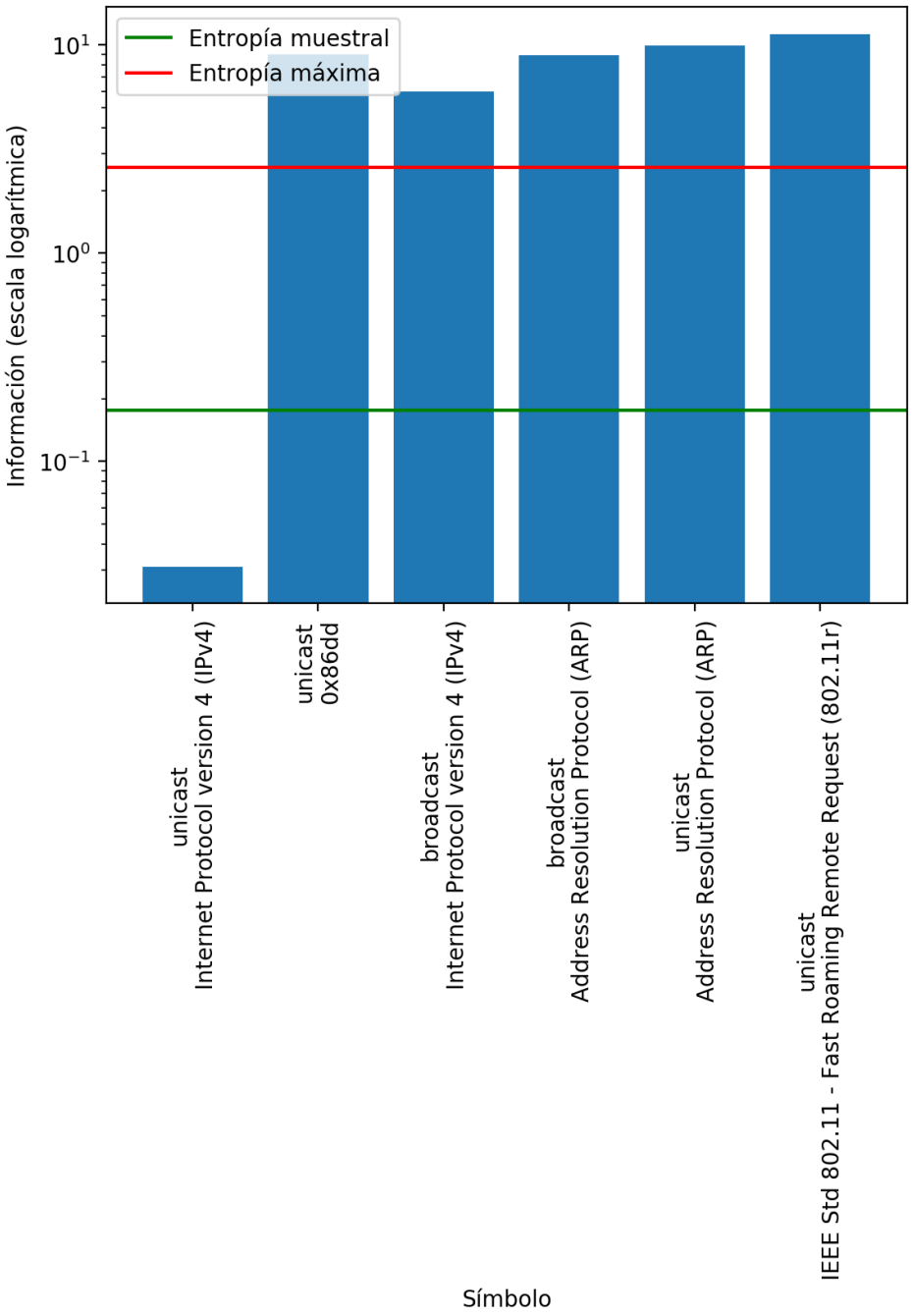

Figura 8: Gráfico de la información de los símbolos de la fuente S_1 observados en esta red. Se muestra la entropía muestral de S_1 y su entropía máxima.

En el caso de la fuente S_2, como podemos ver en la figura 9, hay dos IPs particulares que aportan menos información que las otras, esto significa que es más común que envíen requests de ARP. En este caso, al aportar todos los símbolos aproximadamente la misma información, la entropía muestral se encuentra cerca de la máxima.

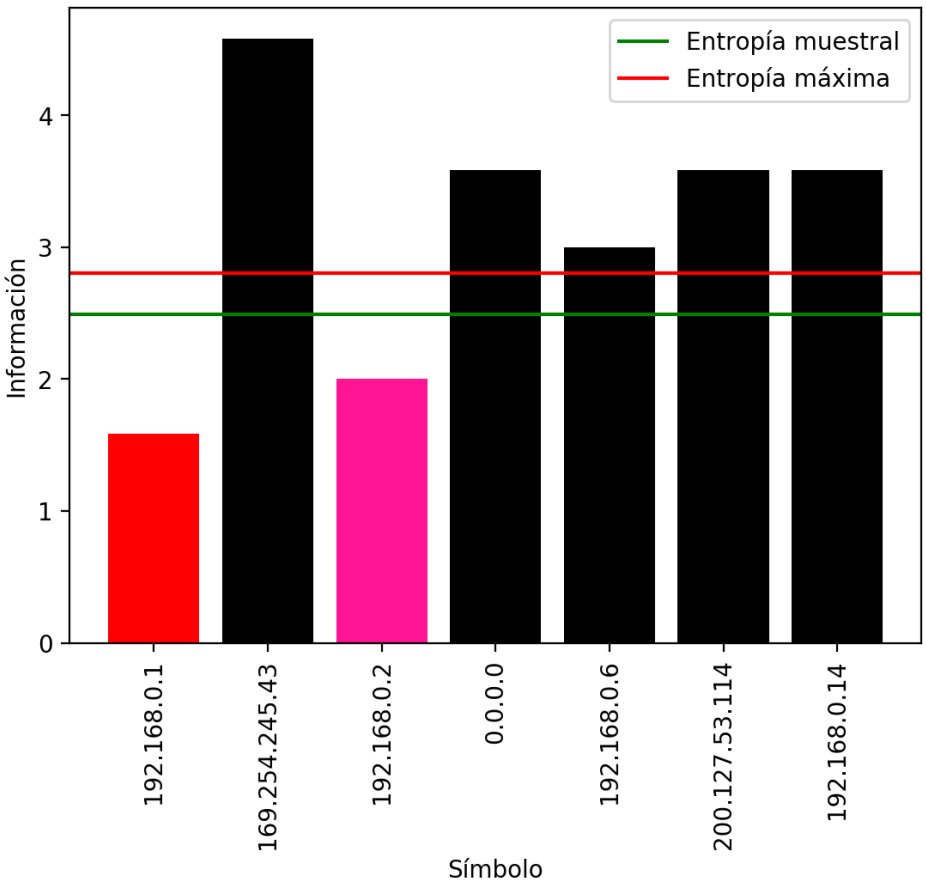

Figura 9: Gráfico de la información de los símbolos de la fuente S_2 observados en esta red. Se muestra la entropía muestral de S_2 y su entropía máxima.

Graficamos la red subyacente de mensajes ARP en la figura 10. Los nodos representan a los hosts y las aristas los mensajes ARP de los dos tipos. No observamos ningún nodo particularmente distinguido.

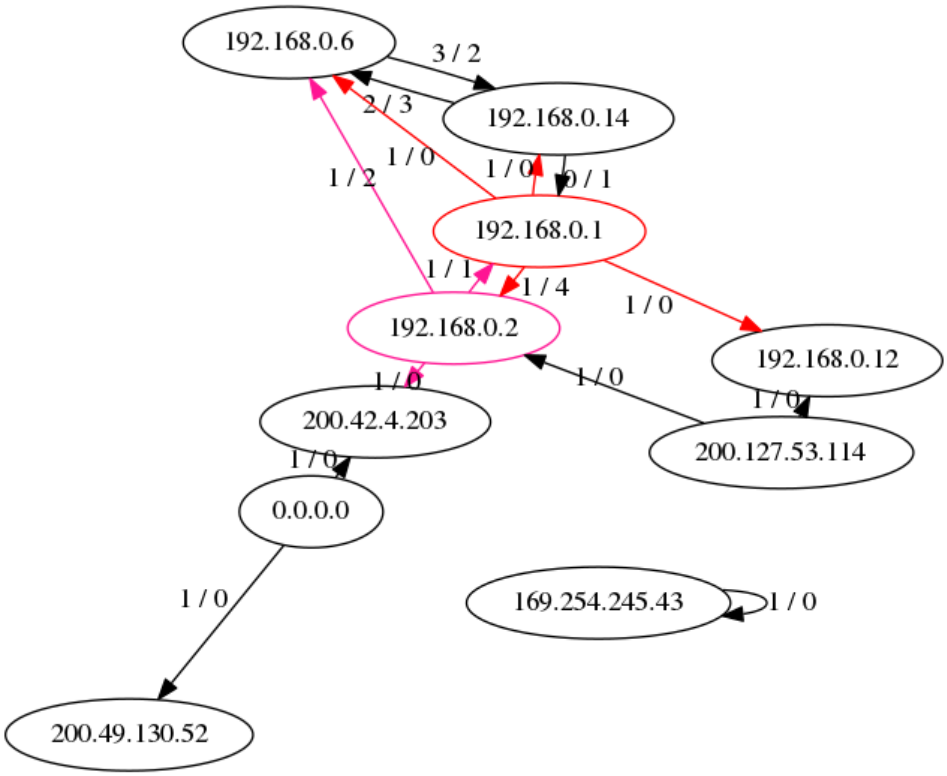

Figura 10: Grafo de la red de mensajes ARP subyacente. Los nodos son las IPs observadas y los ejes son los mensajes ARP. En rojo se marcan los nodos distinguidos (información por debajo de la entropía) y sus mensajes salientes. Cada arista tiene anotada la cantidad de requests/replies ARP.

6. Experimento 3: Red hogareña cableada

6.1. Descripción del contexto

El experimento fue realizado en una red doméstica, por medio de una conexión Wi-Fi. Al momento de tomar las mediciones estaban conectados a la red varias laptops y celulares. La fecha de la captura fue Domingo 8 de Octubre de 2017.

6.2. Descripción de la captura

Capturamos 11000 paquetes. En la figura 11 se muestra la distribución de los protocolos en la red. Observamos que la mayoría de los paquetes son de tipo IPv4, y muchos menos son de tipo ARP y `0x86dd` (IPv6).

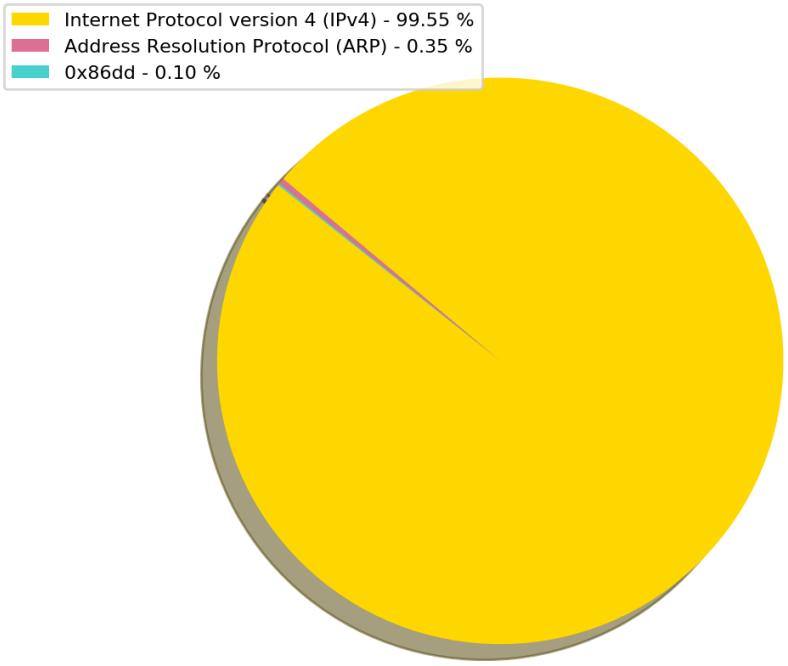

Figura 11: Gráfico que muestra la distribución de protocolos en la red.

En la figura 12 podemos ver el porcentaje de paquetes broadcast comparado con el total de paquetes. Vemos que esto representa un 2,2 % del total. Además, en la figura 13 vemos que los paquetes de broadcast son de tipo IPv4 y ARP.

Este comportamiento es similar al del segundo experimento, ya que ambas son redes domésticas con pocos dispositivos conectados.

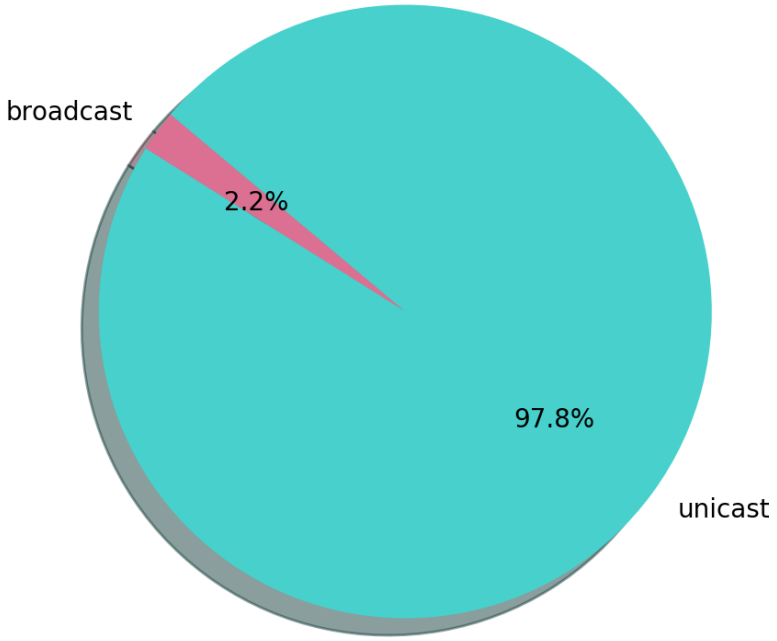

Figura 12: Gráfico que muestra los porcentajes de tráfico broadcast y unicast.

6.3. Análisis de la captura

En la figura 13 se muestra la información de cada símbolo de la fuente S_1. Hay un símbolo con mucha menor información que los demás (IPv4, unicast), se debe a que la mayoría de los paquetes fueron de este tipo. A causa de

esto, la entropía de la fuente es muy baja, está muy lejos del máximo, porque hay grandes diferencias entre el símbolo de menor información y los demás.

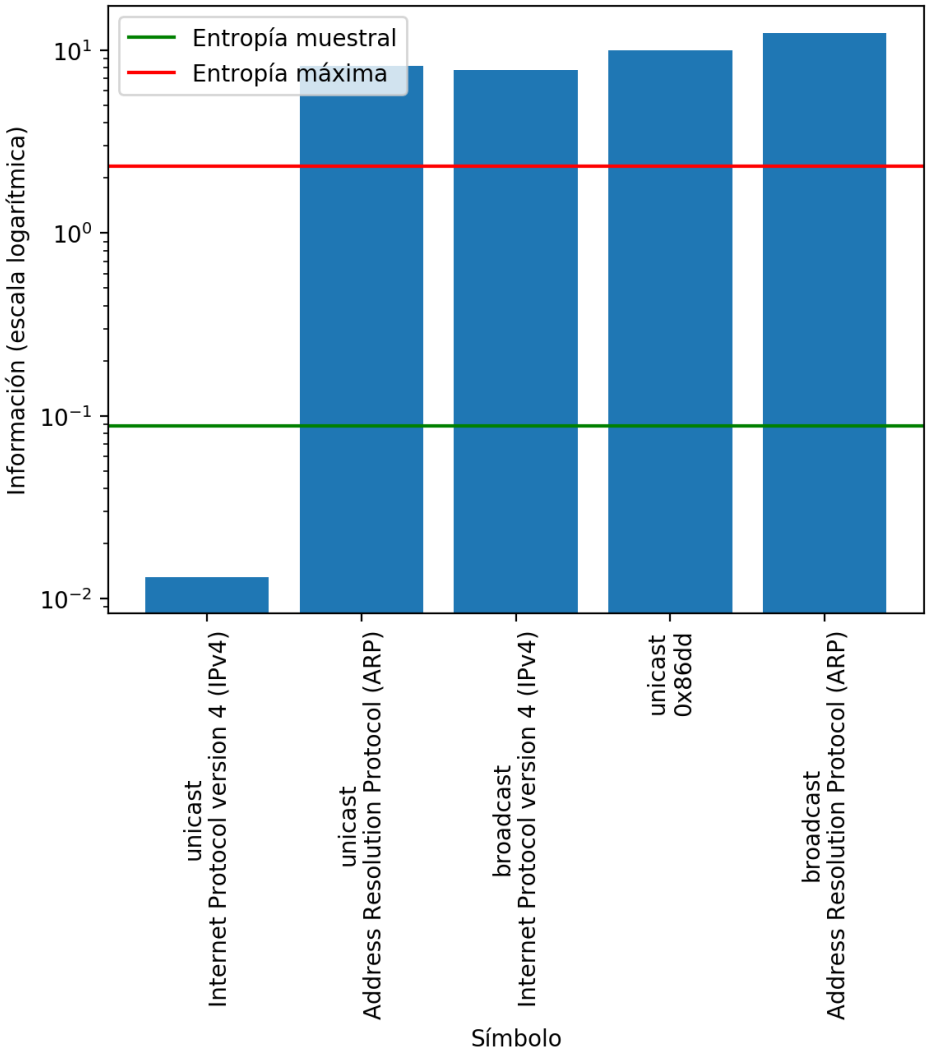

Figura 13: Gráfico de la información de los símbolos de la fuente S_1 observados en esta red. Se muestra la entropía muestral de S_1 y su entropía máxima.

En cuanto a la fuente S_2, vemos en la figura 14 que sólo hay dos símbolos. La red es tan chica que hay solo dos IPs que realizaron request de ARP. La entropía muestral está cerca de $\frac{1}{2}$, la mitad que la entropía máxima.

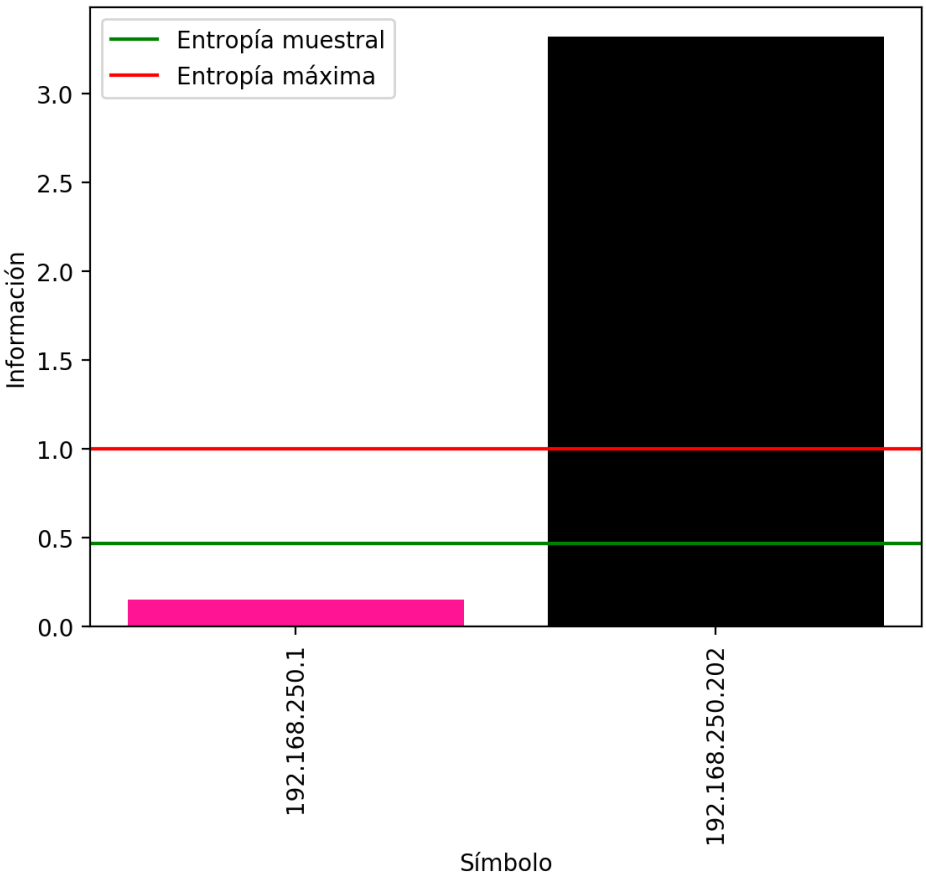

Figura 14: Gráfico de la información de los símbolos de la fuente S_2 observados en esta red. Se muestra la entropía muestral de S_2 y su entropía máxima.

Por último graficamos la red subyacente de mensajes ARP, al igual que en los otros dos experimentos. Observamos que el grafo no es conexo, y no podemos identificar al router. Esto es consistente con el hecho de que no se midieron muchos paquetes ARP en total en esta red.

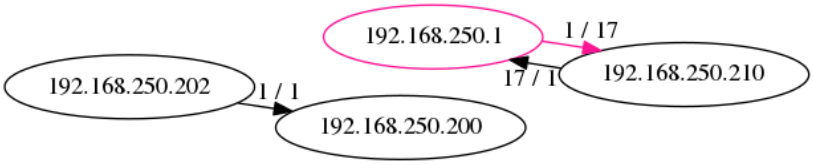

Figura 15: Grafo de la red de mensajes ARP subyacente. Los nodos son las IPs observadas y los ejes son los mensajes ARP. En rojo se marcan los nodos distinguidos (información por debajo de la entropía) y sus mensajes salientes. Cada arista tiene anotada la cantidad de requests/replies ARP.

7. Conclusiones

Lo primero que pudimos observar, es que en todos los experimentos había una proporción muy grande de paquetes <unicast, ipv4>. Esto se debe a que en todos los casos, el uso principal de la red es acceder a internet, de ahí el gran intercambio de paquetes de este tipo. Pero otra parte pudimos observar que la proporción de paquetes broadcast en todos los casos fue menor a la de paquetes unicast. Esto puede deberse a que los paquetes broadcast se utilizan para obtener información acerca de la red o para informar cambios en la misma. Ya que los cambios no son frecuentes (al menos en los casos analizados) y, en consecuencia, la información que se obtiene de la red puede ser reutilizada, podemos concluir que no hay mucha necesidad de utilizar muchos paquetes de tipo broadcast.
Por último, pudimos observar un comportamiento muy similar en las dos redes hogareñas, con la excepción de que la red conectada por cable detectaba menos paquetes ARP. Esto puede deberse a que lo que se observa desde una conección wifi tiene una naturaleza mas "volatil"(en todo momento hay dispositivos conectandose y desconectandose de la red) por lo que es normal que se hayan observado mas paquetes de este tipo.