DEPARTAMENTO DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

TP1: Wiretapping

Teoría de las Comunicaciones

Integrante	LU	Correo electrónico
Furman, Damián	936/11	damian.a.furman@gmail.com
Lambrisca, Santiago	274/10	santiagolambrisca@hotmail.com
Marottoli, Daniela	42/10	dani.marottoli@gmail.com
Vanecek, Juan	169-10	juann.vanecek@hotmail.com

Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Ciudad Universitaria - (Pabellón I/Planta Baja)
Intendente Güiraldes 2160 - C1428EGA
Ciudad Autónoma de Buenos Aires - Rep. Argentina
Tel/Fax: (54 11) 4576-3359
http://www.fcen.uba.ar

Índice

1. Introducción

Aprovechando las herramientas existentes para el análisis de transferencia de paquetes, como Scapy y Wireshark, nos desarrollamos nuestra propia herramienta que nos permite captar paquetes los paquetes de la redes local a donde estemos conectados. Para poder realizar esto, tuvimos que valernos de una modalidad de uso brindada por la placa de red.

Asi, utilizando la placa de red en modo Promiscuo o Monitor, nos dispusimos a captar los paquetes correspondientes al protocolo ARP (Address Resolution Protocol), con el objetivo de realizar un análisis sobre el intercambio de paquetes de este protocolo realizado en distintas redes, buscando identificar los nodos más significativos e intentando comprender su rol dentro de la red. Este tipo de paquetes es adecuado para este análisis ya que en redes de acceso múltiple son el encargado de traducir direcciones de red (IP) en direcciones de enlace (MAC). Los hosts los envían cuando quieren conocer la ubicación de cierta IP, y un router está constantemente actualizando su tabla de routeo, por lo que podríamos identificar a estos de acuerdo al flujo de ARPs que corren por la red.

Valiéndonos de distintas herramientas de análisis y graficación hemos realizado este trabajo, obteniendo los resultados y haciendo los análisis presentados a continuación.

2. Desarrollo

En el primer punto nos piden que implementemos una herramienta para escuchar pasivamente una red local. Scapy nos provee una serie de métodos como `sniff` que ejecuta un callback cada vez que la placa de red recibe un paquete. Luego la clase `Sniffer` se encarga de parsearlo si es un paquete ARP, y guardarlo convenientemente.

El paquete esta compuesto, entre otras cosas, por la dirección IP y MAC origen y destino, y el tipo de consulta: *who-has* o *is-at*.

Como método para identificar los routers en la red analizamos tres fuentes de información en 5 redes diferentes (2 domésticas, 2 empresariales, 1 pública). Las fuentes que usamos fueron:

1. *IP origen*; evento: IP X manda un paquete *who-has*.
2. *IP destino*; evento: IP X recibe un paquete *who-has*.
3. *IP origen - IP destino*; evento: IP X manda un paquete who-has a y.

Para cada una de estas fuentes, la clase `Sniffer` contiene un diccionario para almacenar cada evento.

Una vez que ya tenemos la estructura armada, pusimos a correr el programa unos 30 minutos en cada LAN, un tiempo que consideramos prudente para poder tomar conclusiones.

Como queremos encontrar los puntos distinguidos en la red, nosotros los vamos a considerar a partir de los eventos que posean menos información o, lo que es lo mismo, que tengan una mayor probabilidad de que suceda. En particular, nos interesan los eventos s que cumplan $I(s) - H(S) < 0$.

3. Gráficos y análisis

Para las distintas redes utilizadas, presentamos los datos obtenidos a traves de distintos gráficos, uno para cada fuente de información considerada, que nos permiten, no solo mostrar mas claramente los resultados obtenidos, sino que también son útiles para realizar el analisis de las distintas redes y compararlas entre si.

Consideramos de utilidad, para analizar las fuentes de información 1y 2 presentadas en el desarrollo, representar la actividad mostrada por cada nodo dentro de una red graficando la

cantidad de información proporcionada por el evento relacionado a este. Además decidimos mostrar una linea color rojo que representa la Entropia de la red. El echo de que la información brindada por un nodo se encuentre debajo de la linea roja, nos indica que ese nodo tiene una actividad significativa dentro de la red y nos dice que dicho nodo es de importancia a la hora de realizar el analisis.

Por otro lado, para el analisis de la fuente de información 3, presentamos un grafo, con nodos de distintos tamaños, donde los nodos representan una IP y los ejes un un paquete que lo referencia como destino o fuente segun la dirección. El tamaño de los nodos representa la cantidad de intercambios en los que participo, viendose asi, los nodos mas significativos graficados con mayor tamaño y siendo facilmente identificables.

3.1. Red WiFi casa particular 1

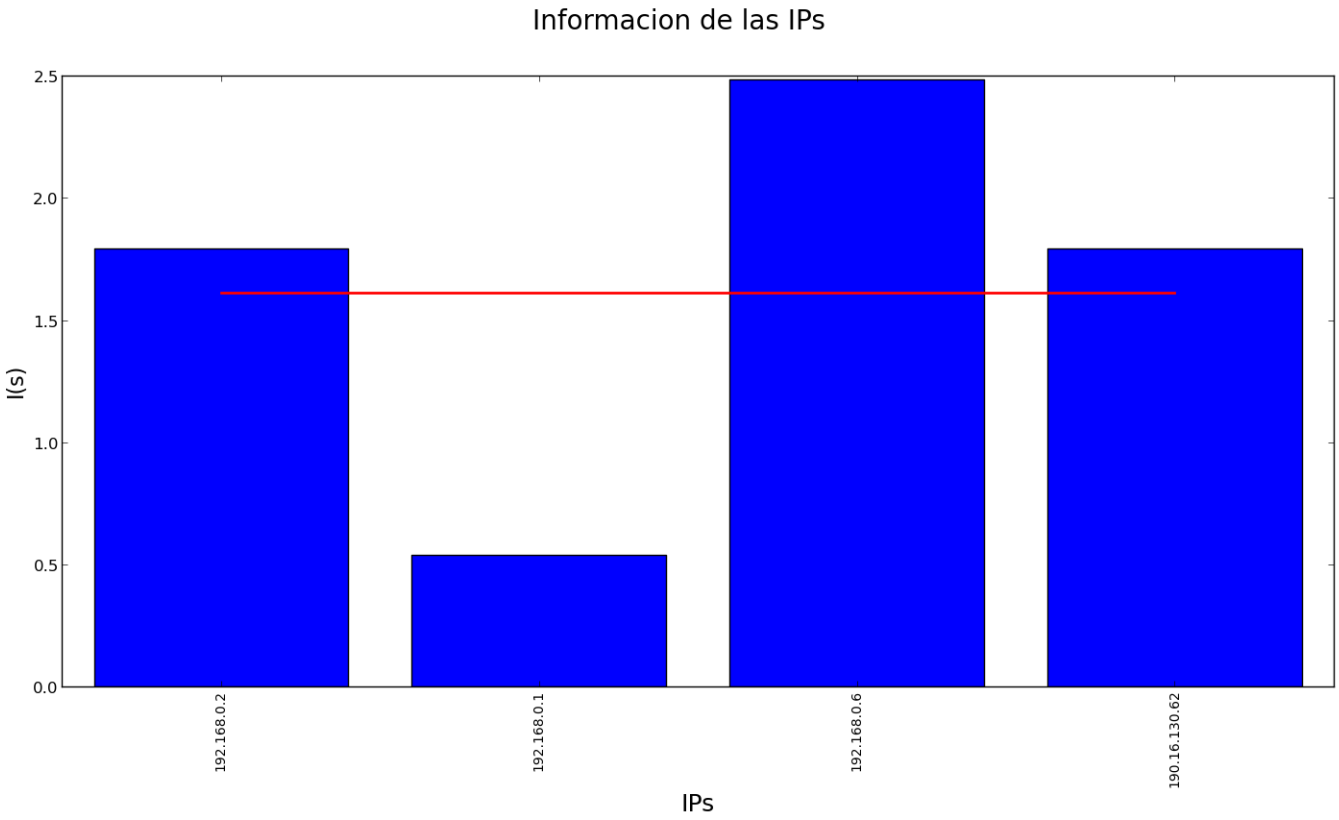

Figura 1: Fuente de información: IPs que envían

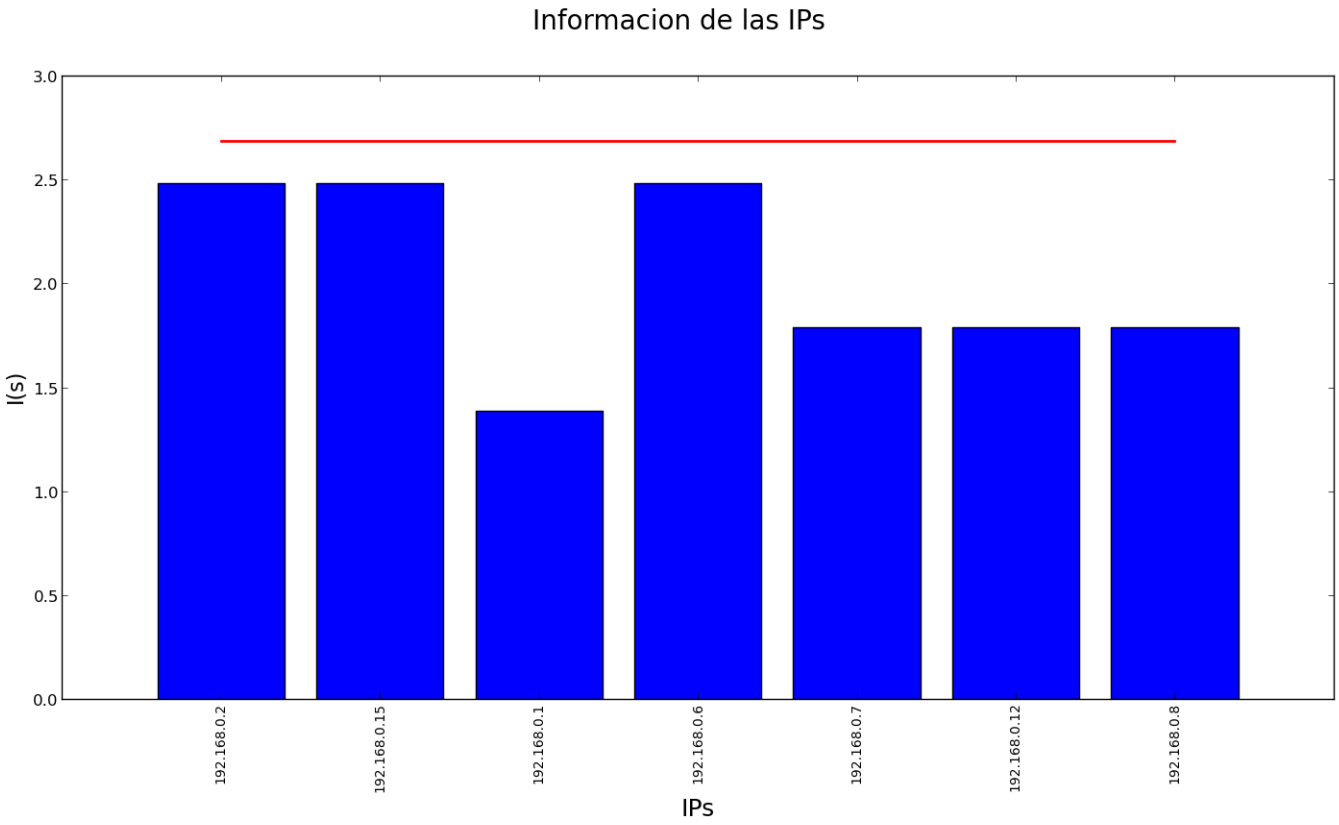

Figura 2: Fuente de información: IPs que reciben

Los gráficos presentados anteriormente pertenecen a una casa particular. Podemos observar que uno de los nodos de la red representa una cantidad de unidades de información notablemente menor a la de los demás. Siendo que la función que determina las unidades de información para cada evento, es decreciente, mientras mas veces haya ocurrido este evento en el periódo de tiempo que se tomó la muestra, menor será la cantidad de información que representa el echo que ese evento ocurra. Asi, vemos que el evento cuya información se destaca por ser notablemente menor a los demas, es el que más intercambio de paquetes ha realizado. Tentados a pensar que este deberia ser el nodo de la red que representa al Router, pudimos comprobarlo en la configuración de la red. Otro indicio fácil de notar habia sido la dirección IP asociada a este nodo (192.168.0.1)

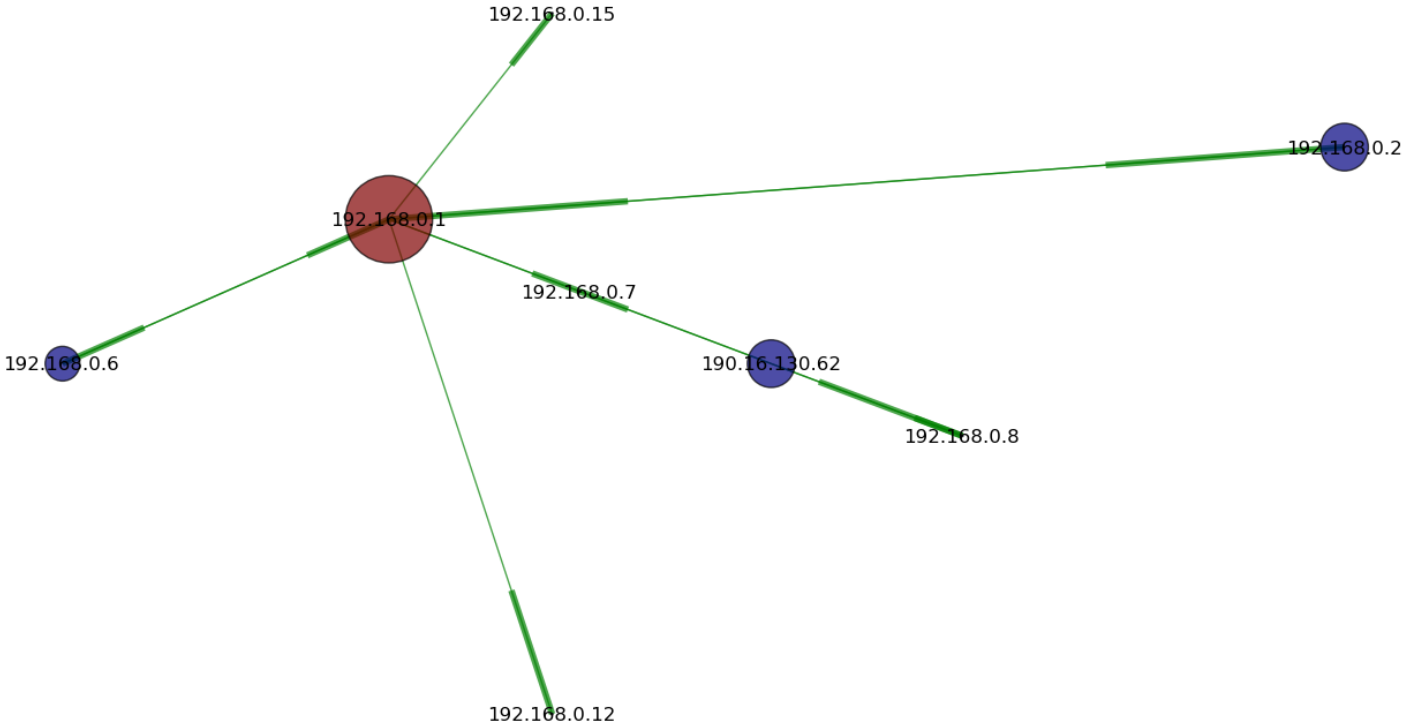

Figura 3: Red WiFi casa doméstica 1

En este gráfico, podemos identificar claramente a un nodo con gran actividad dentro de la red, coherentemente con los gráficos anteriores, es nuevamente en este gráfico el nodo (192.168.0.1) es el de mayor actividad dentro de la red, correspondiendose esta direccion con la del Router.

3.2. Red WiFi casa particular 2

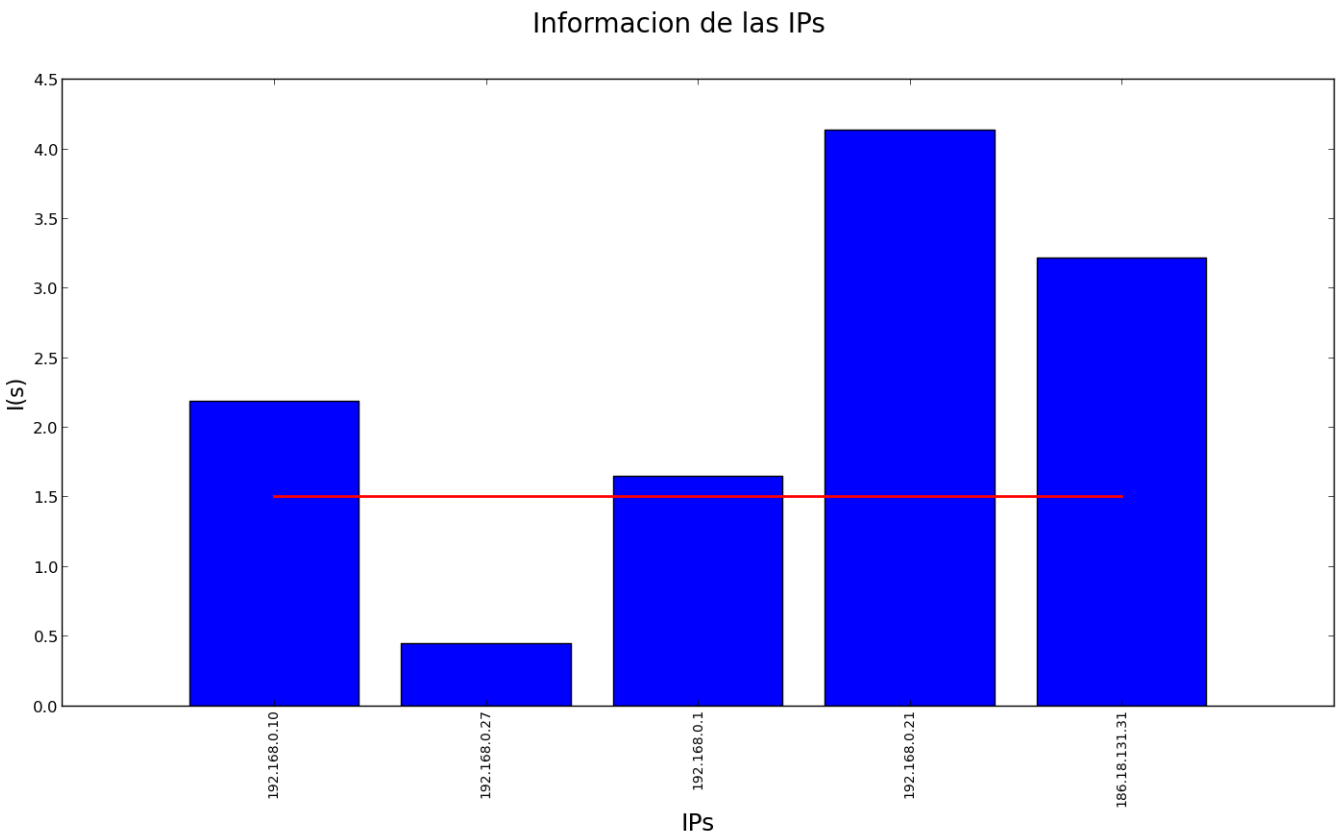

Figura 4: Fuente de información: IPs que envían

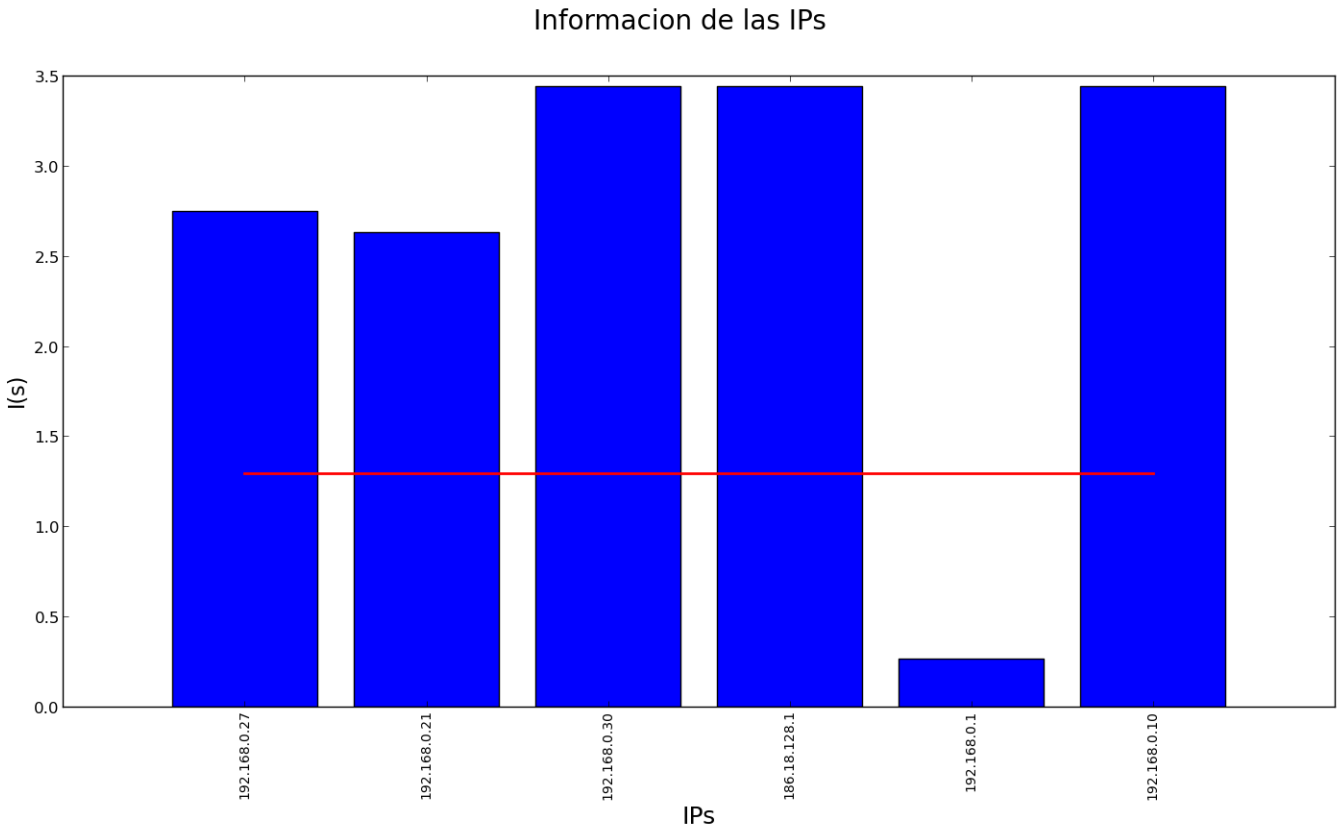

Figura 5: Fuente de información: IPs que reciben

Estos gráficos se corresponden con otra red de una casa. Sin embargo, nos da la posibilidad algunos resultados que no estabamos esperando. En el primer gráfico nos encontramos con un evento distinguido, el cual se corresponde con la IP 192.168.0.27, sin embargo, si miramos el segundo gráfico el evento distinguido se corresponde con otra direccion IP, la 192.168.0.1. esto nos p'lantea un interrogante sobre cual se corresponde al Router, nuestros conocimientos previos nos llevan a pensar que la segunda direccion se corresponde con el Router, y nos encargamos de chequearlo. La duda paso a ser, a que host pertenecia la otra IP. Nos encontramos con que esta IP se corresponde al Servidor Web, Apache, utilizado localmente.

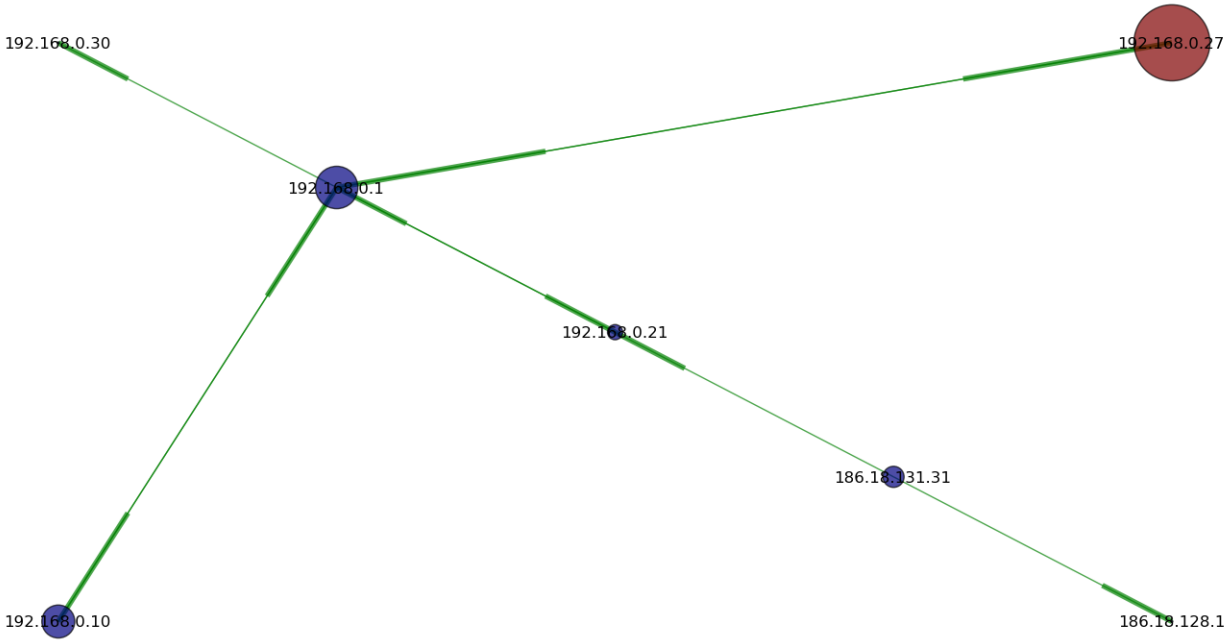

Figura 6: Red WiFi casa doméstica 2

Nuevamente, y coherentemente con lo mostrado en los gráficos anteriores, nos encontramos con un nodo significativo, pero que no se corresponde con el Router, sino con el Servidor Web. Sin embargo, debido a la cantidad de aristas con las que se conecta uno de los nodos, nos permite pensar que ese es el Router y lo comprobamos ya que su IP es 192.168.0.1

3.3. Red Ethernet Empresa 1 (Recursiva)

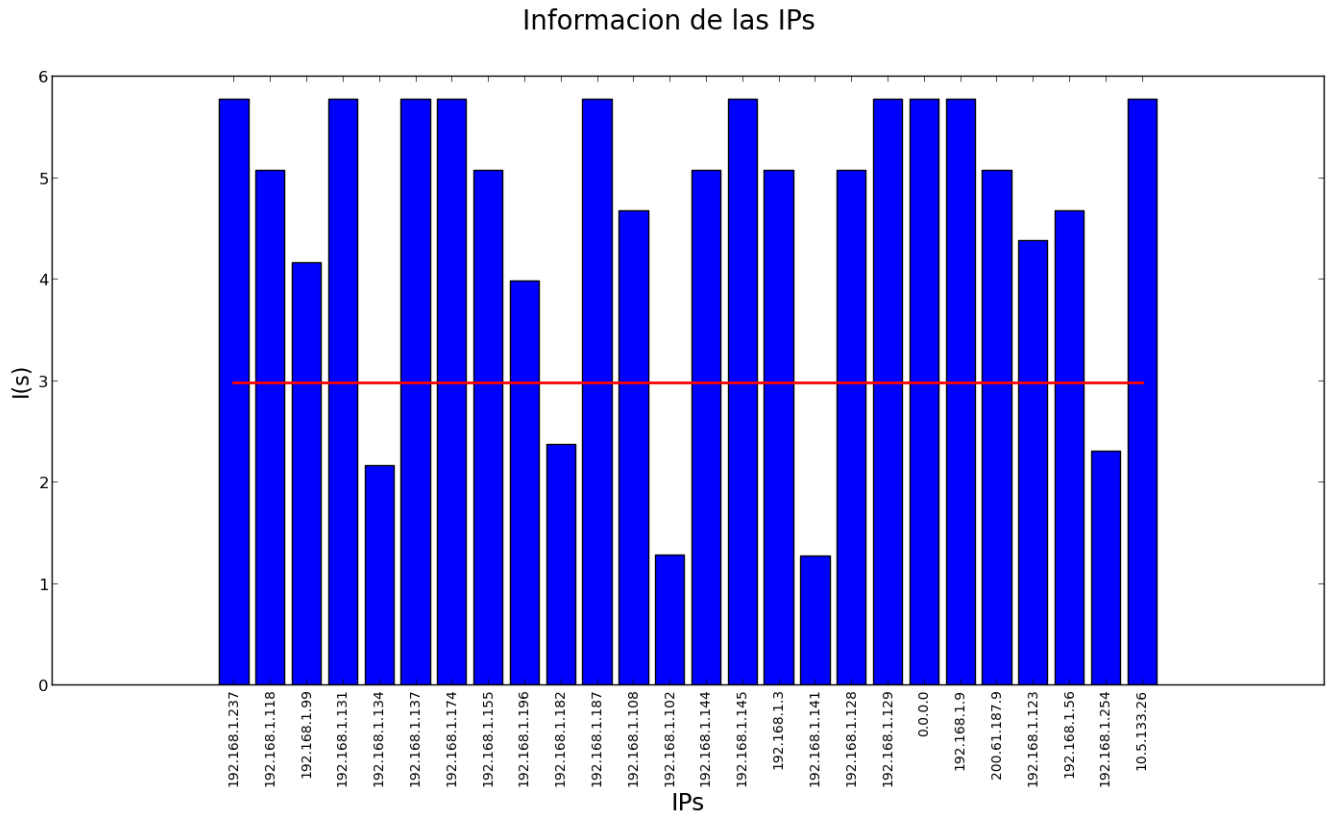

Figura 7: Fuente de información: IPs que envían

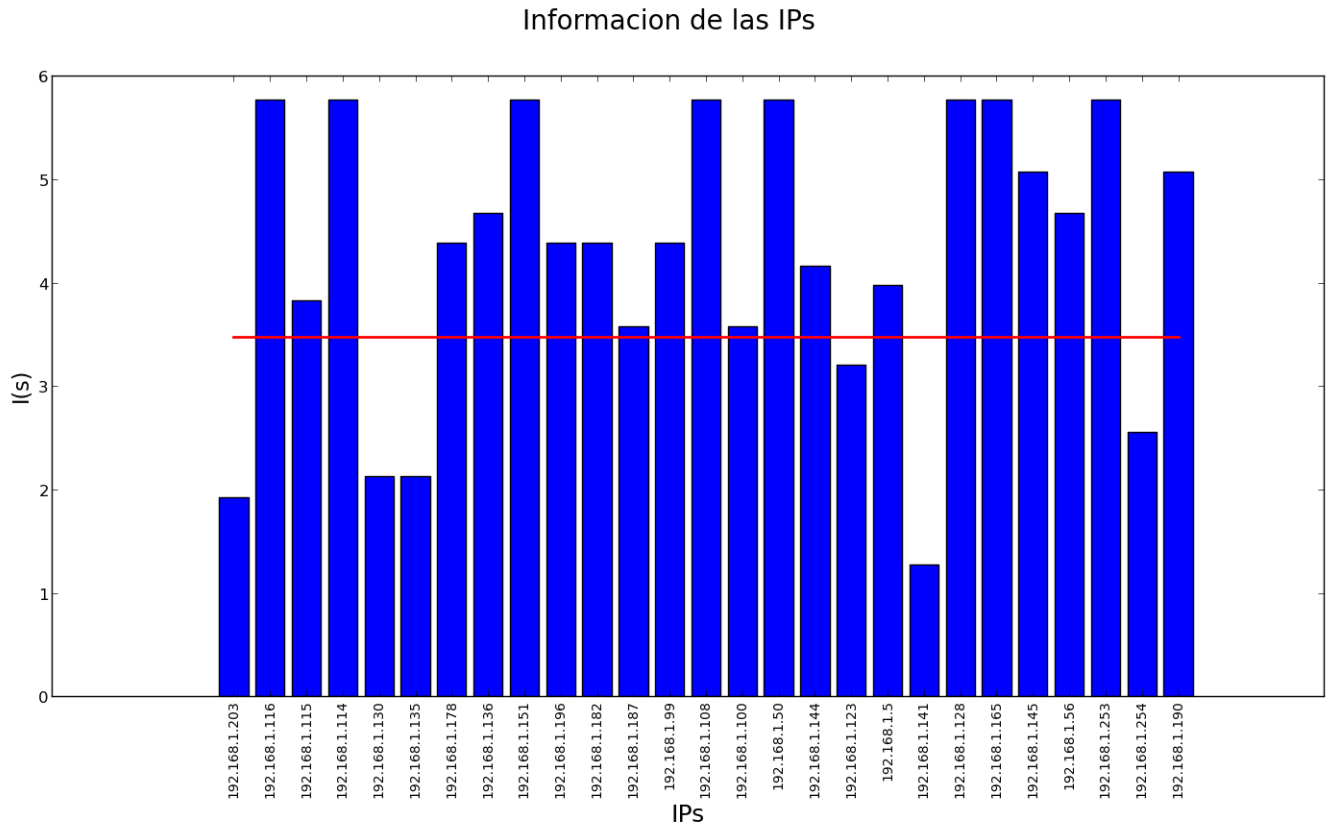

Figura 8: Fuente de información: IPs que reciben

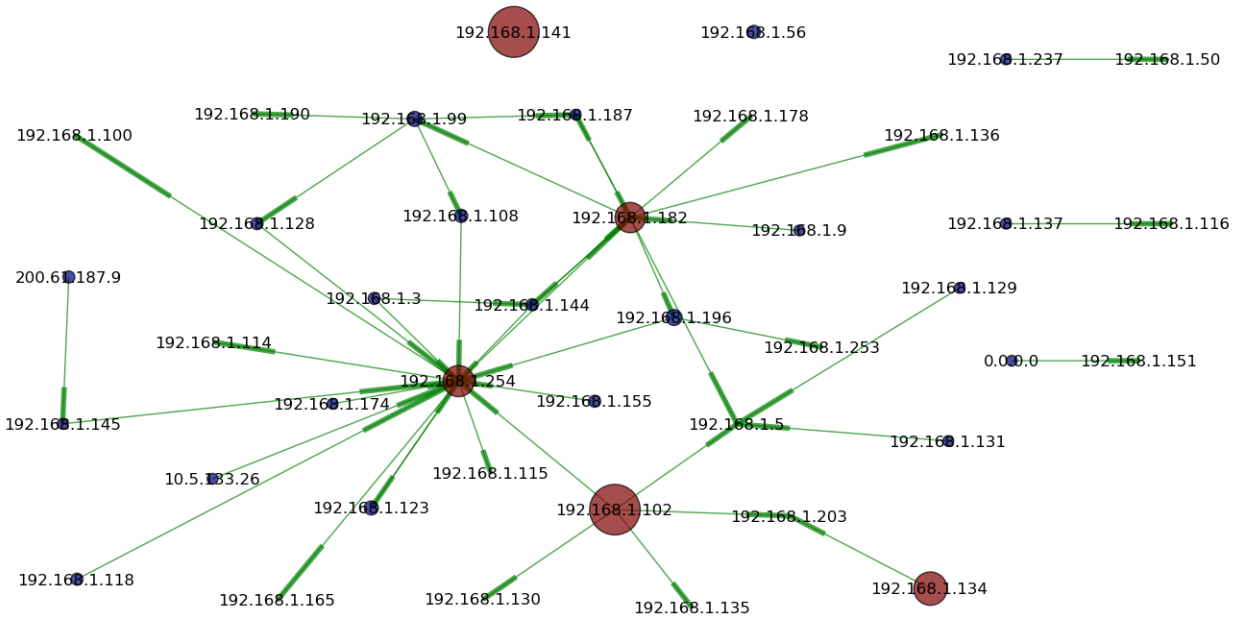

Figura 9: Red Ethernet de Recursiva

3.4. Red Ethernet Empresa 2 (ORSNA)

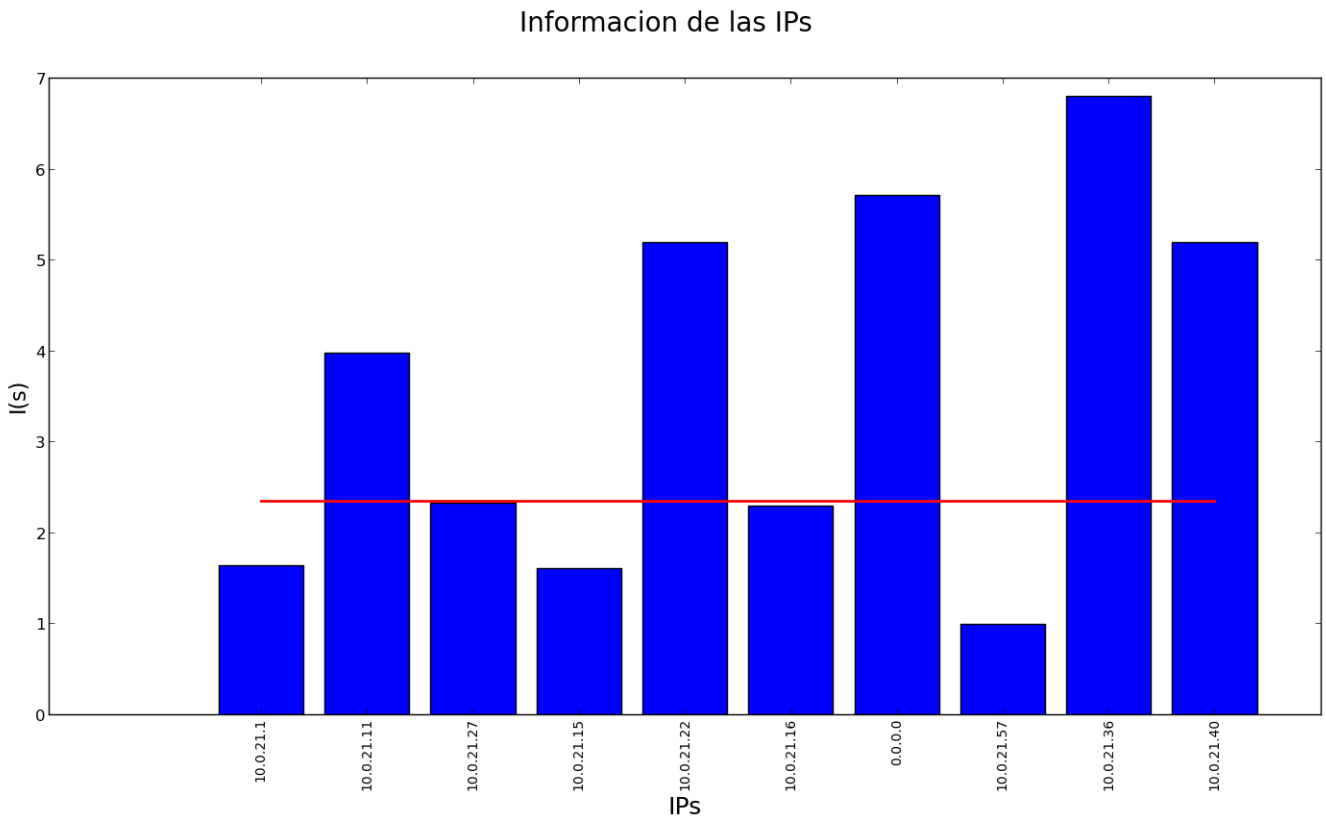

Figura 10: Fuente de información: IPs que envían

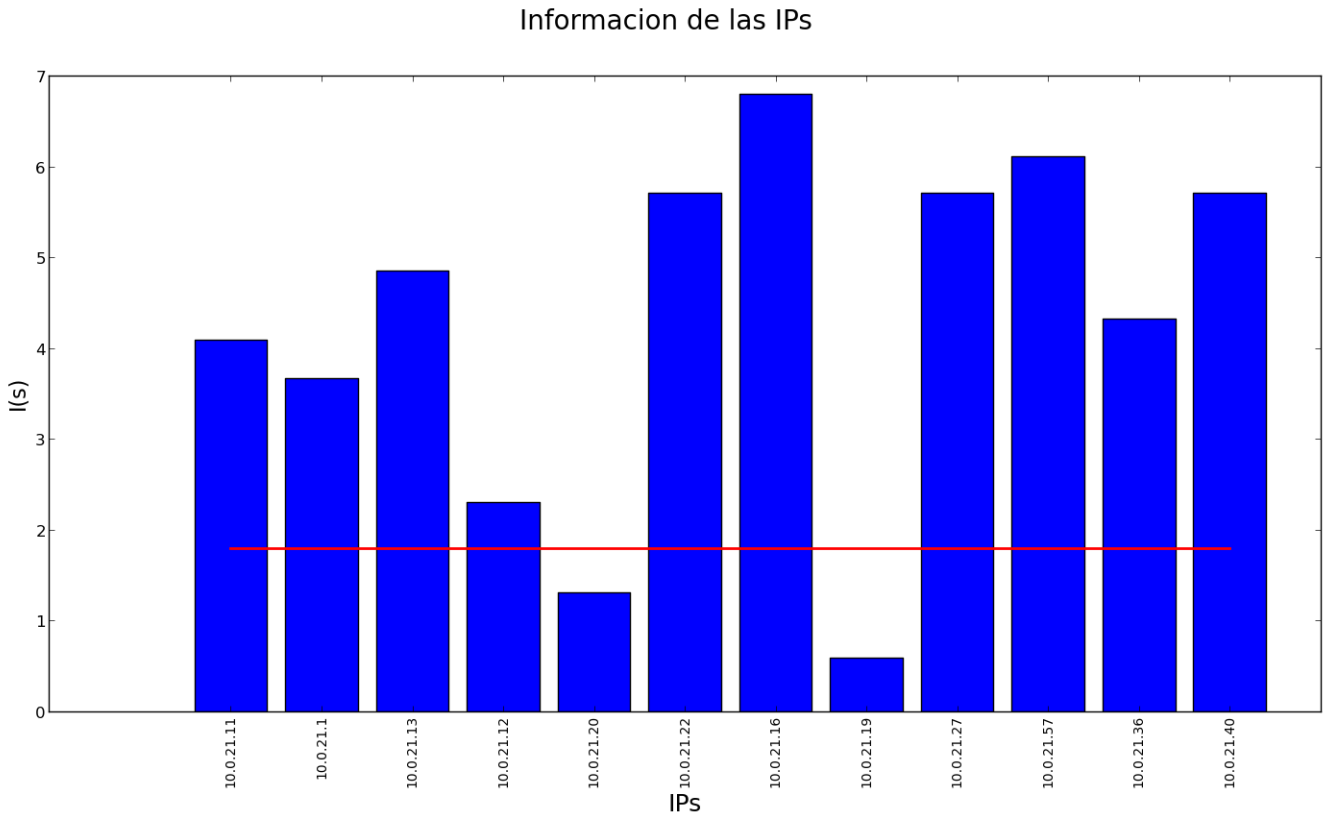

Figura 11: Fuente de información: IPs que reciben

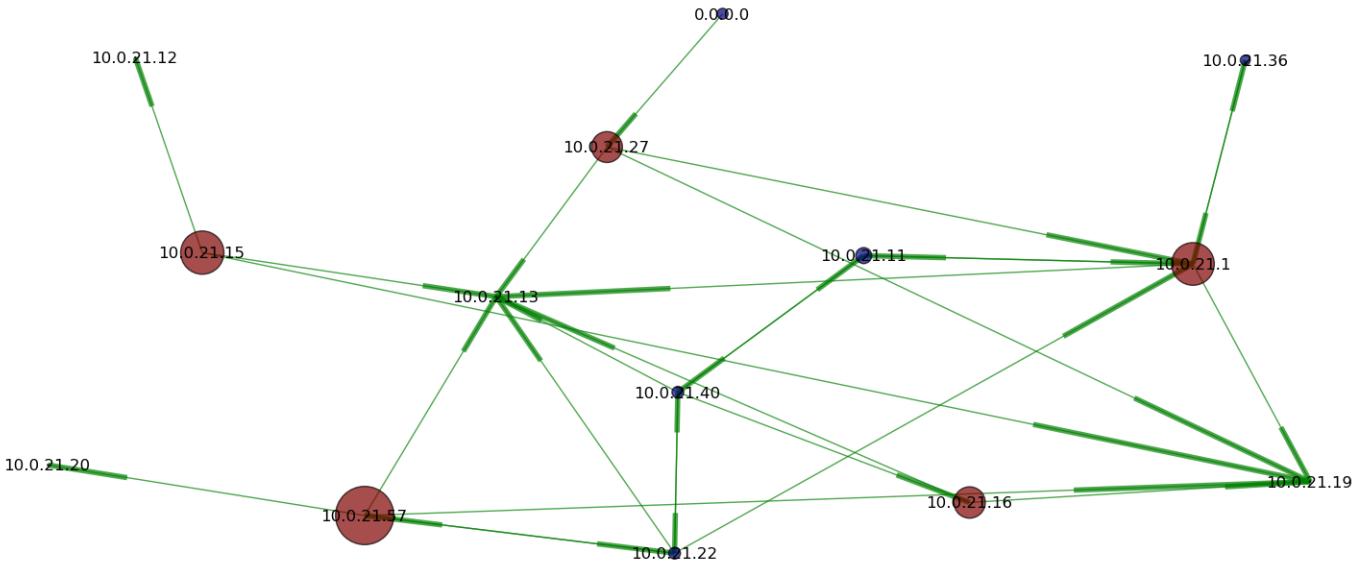

Figura 12: Red Ethernet de ORSNA

3.5. Red WiFi local comercial (McDonalds)

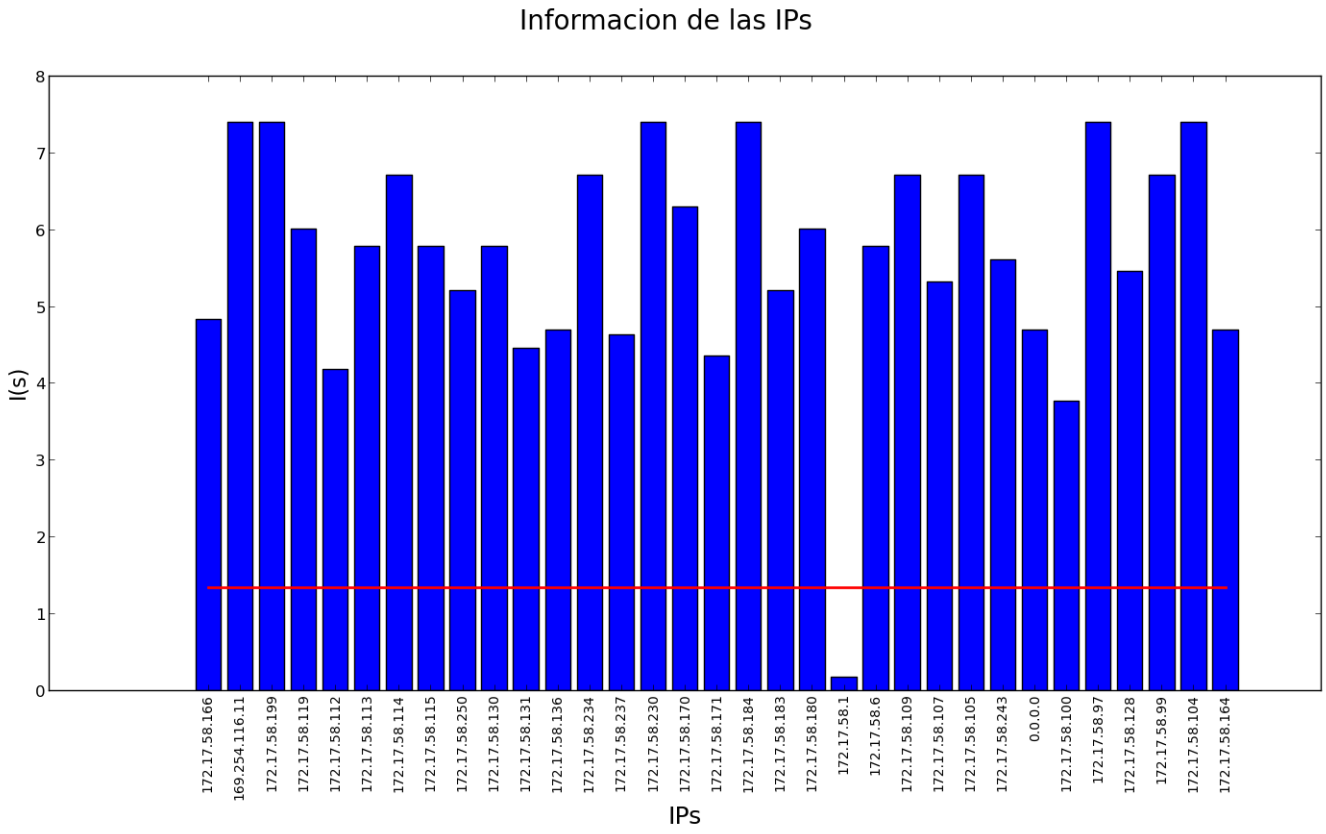

Figura 13: Fuente de información: IPs que envían

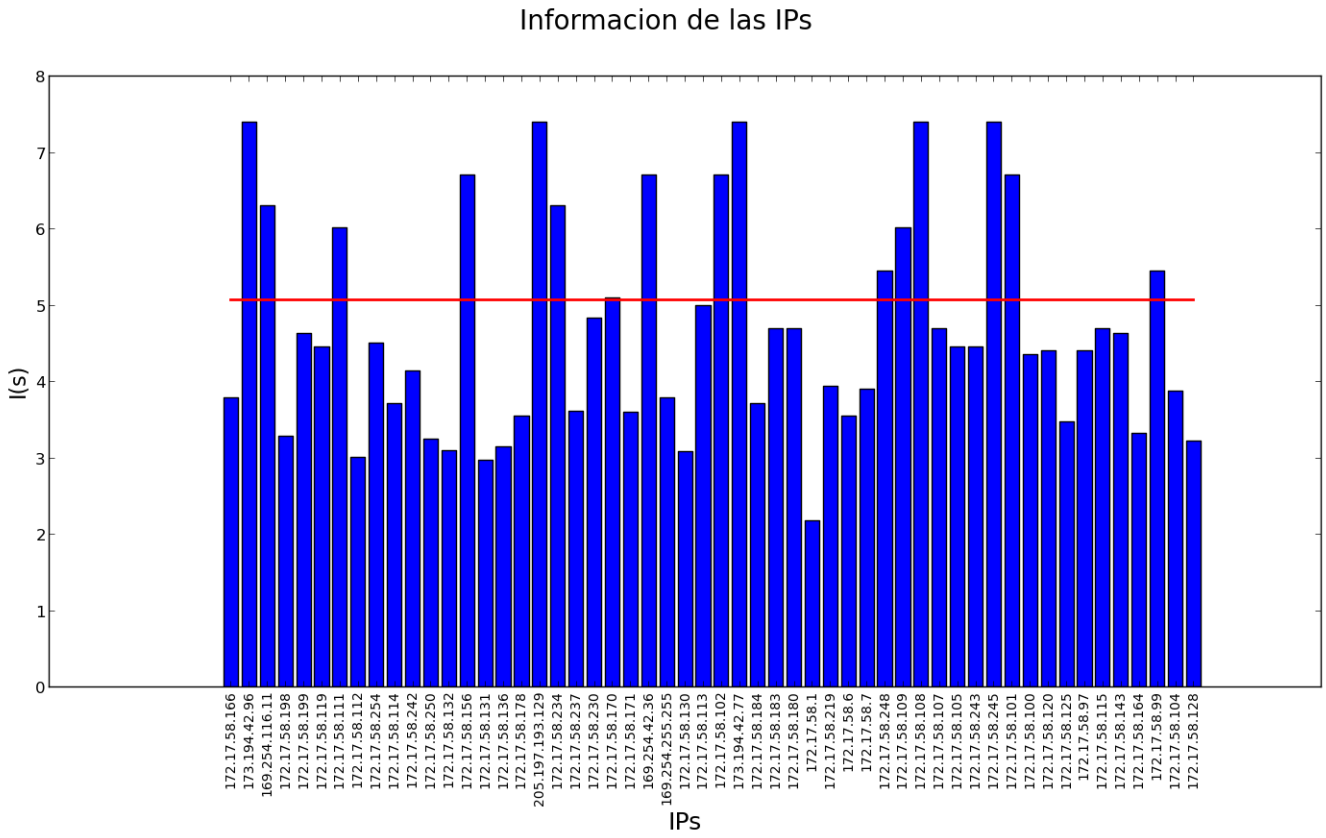

Figura 14: Fuente de información: IPs que reciben

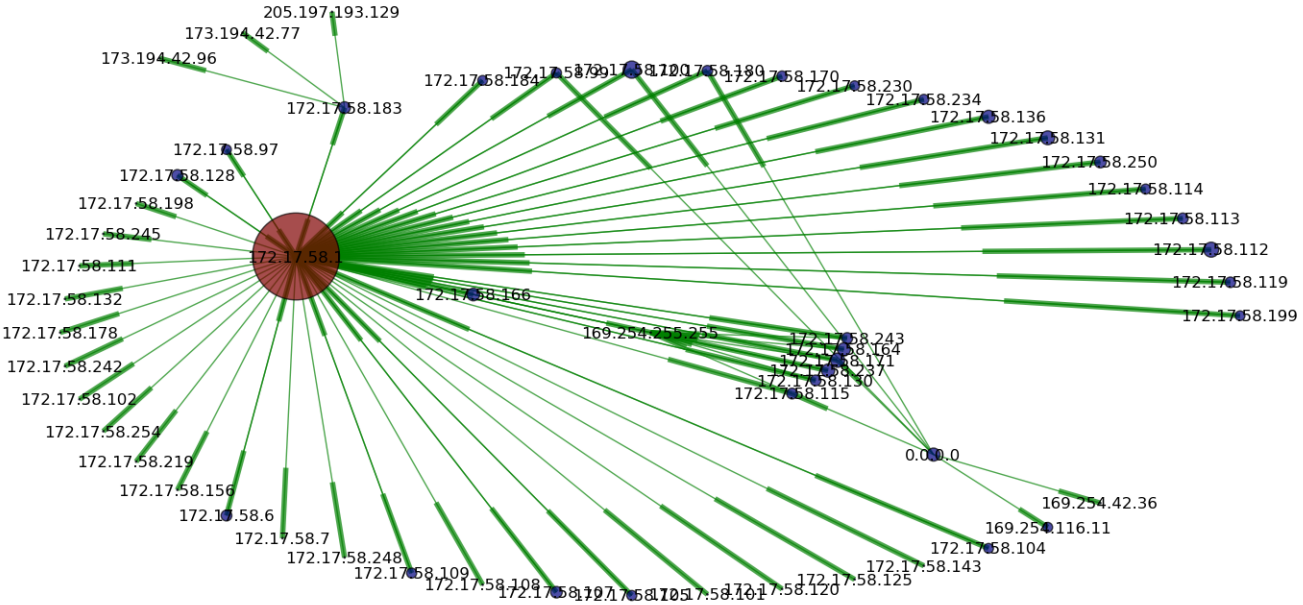

Figura 15: Red WiFi de McDonalds

4. Conclusiones