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 eventos.

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 poseamos menos información o, lo que es lo mismo, que tengan una mayor probabilidad de que suceda. En particular, a los eventos s que cumplan $I(s) - H(S) < 0$.

3. Gráficos y análisis

3.1. Red WiFi casa particular 1

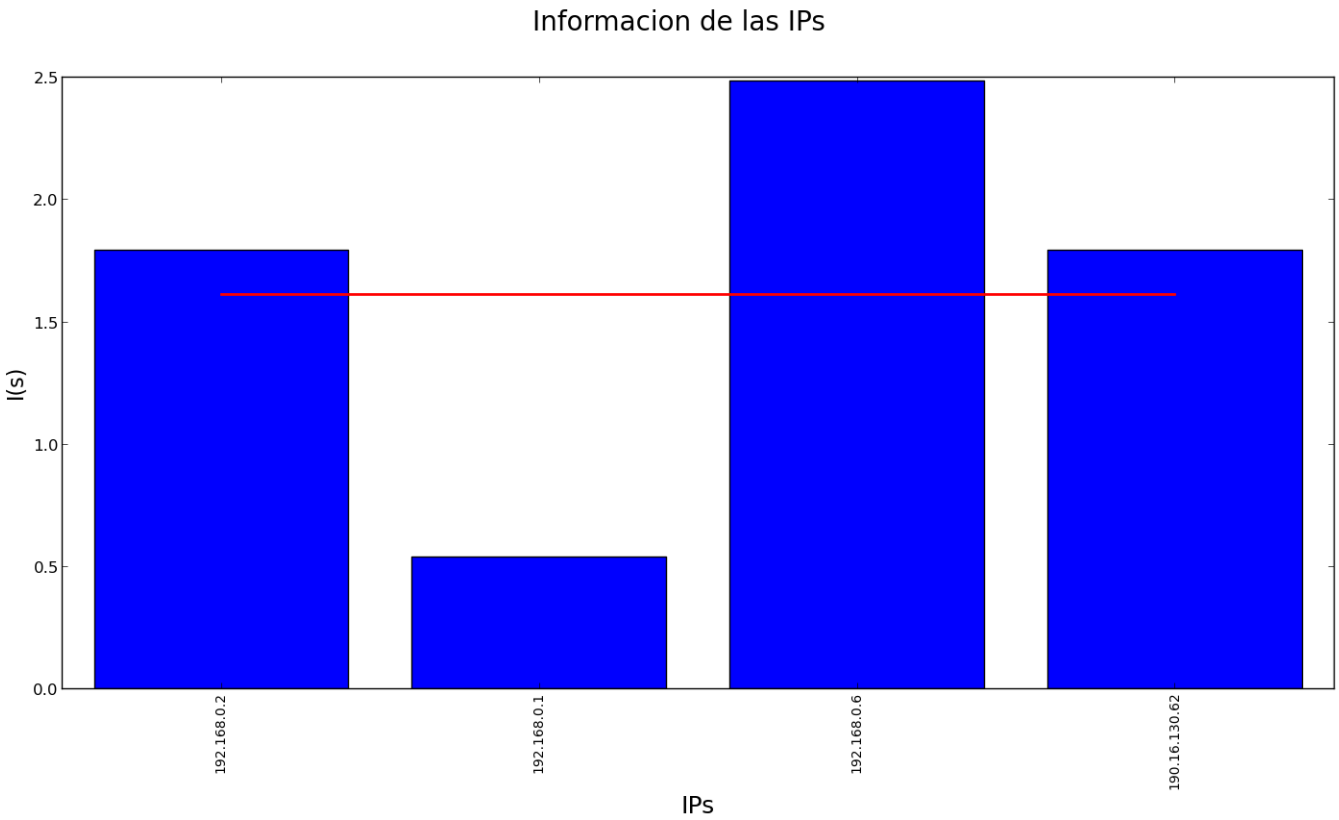

Figura 1: Fuente de información: IPs que envían

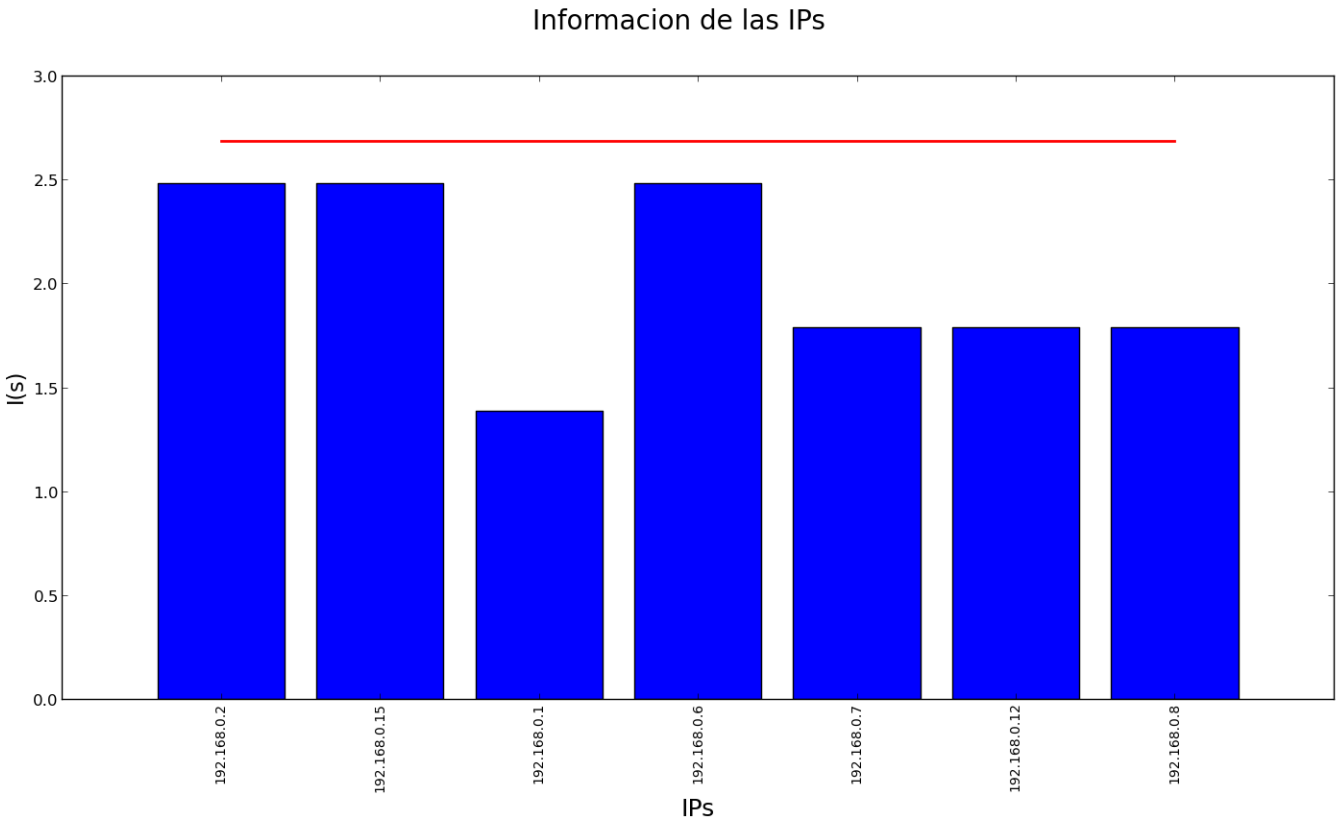

Figura 2: Fuente de información: IPs que reciben

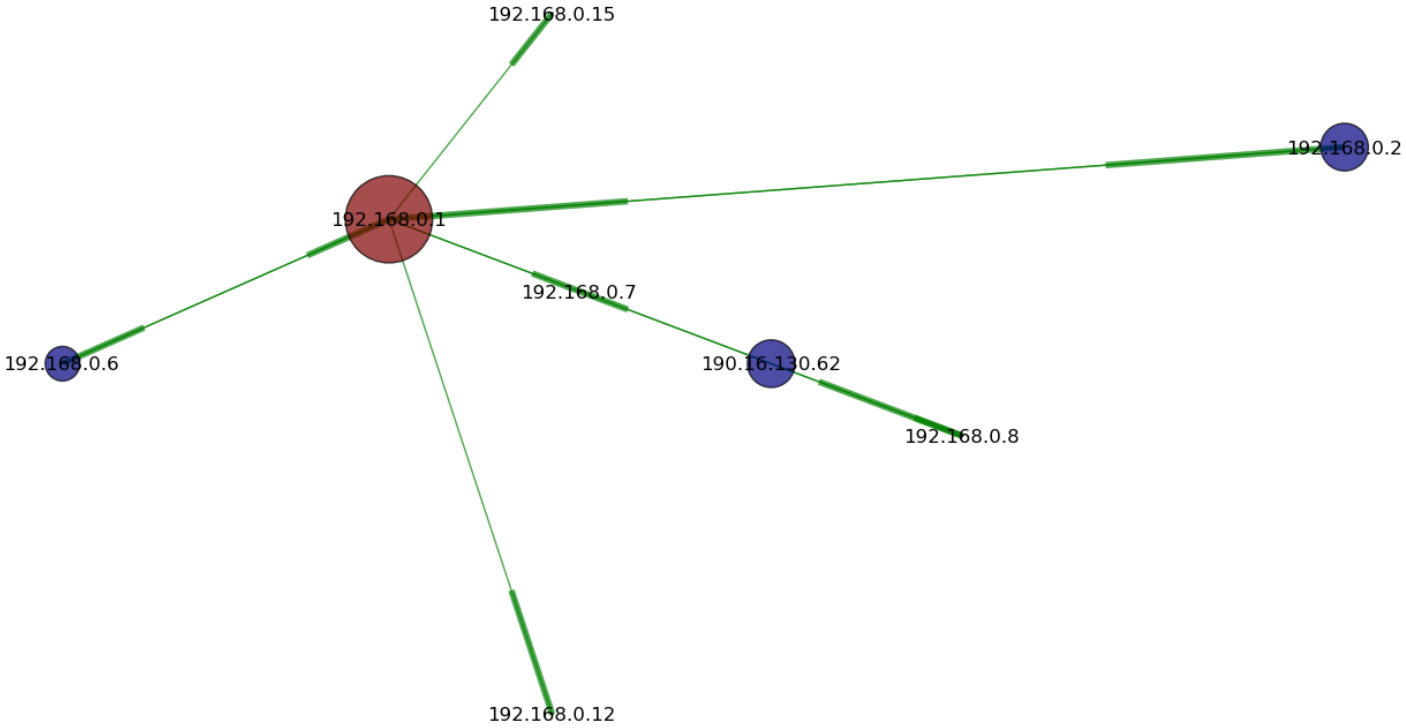

Figura 3: Red WiFi casa doméstica 1

3.2. Red WiFi casa particular 2

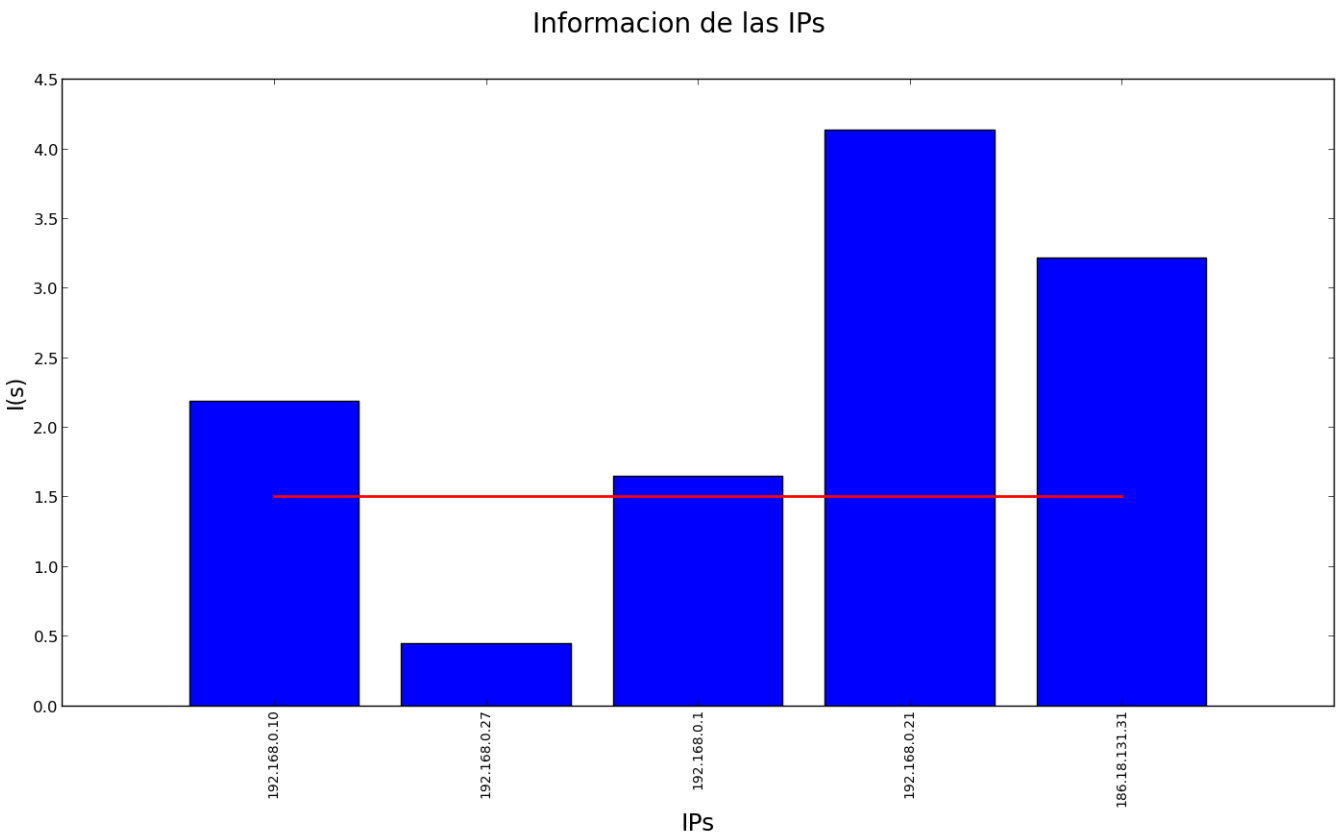

Figura 4: Fuente de información: IPs que envían

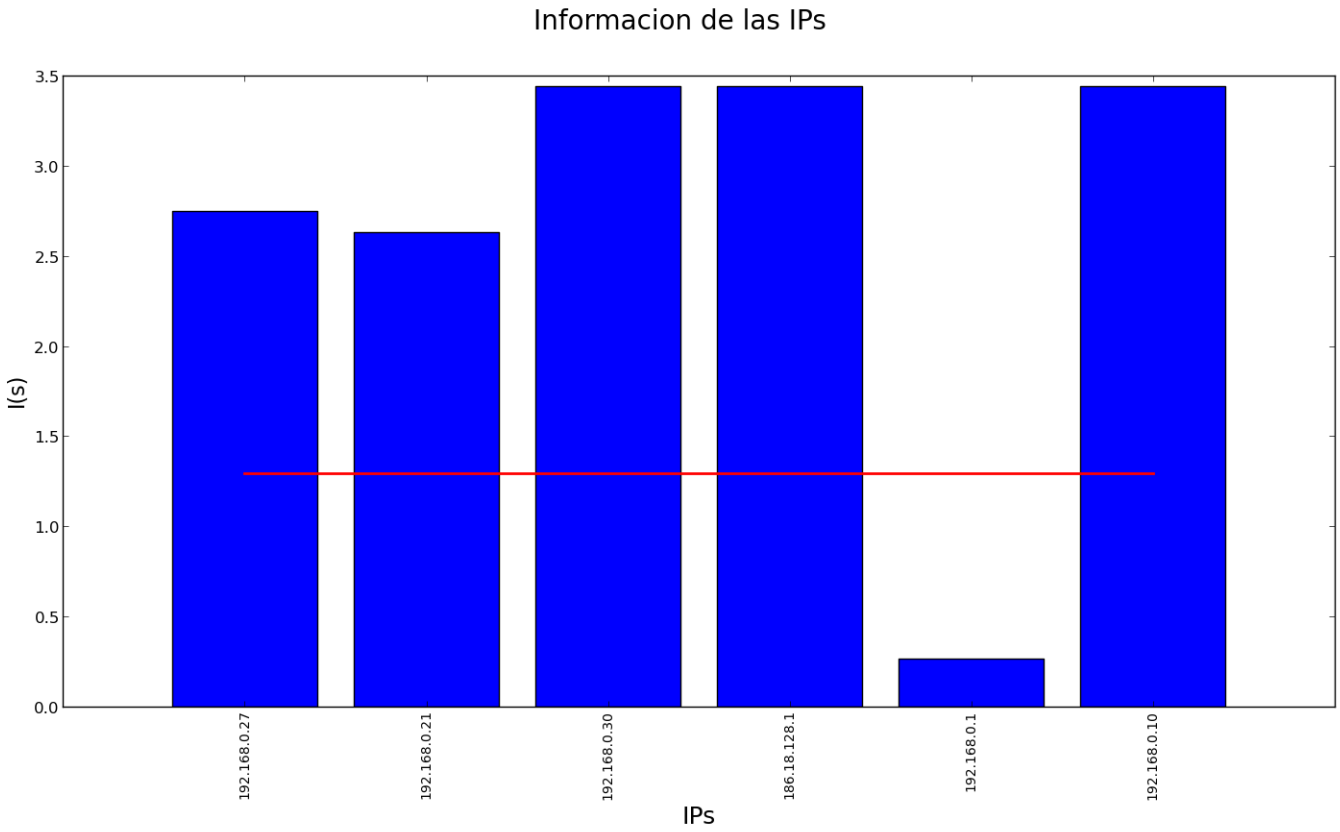

Figura 5: Fuente de información: IPs que reciben

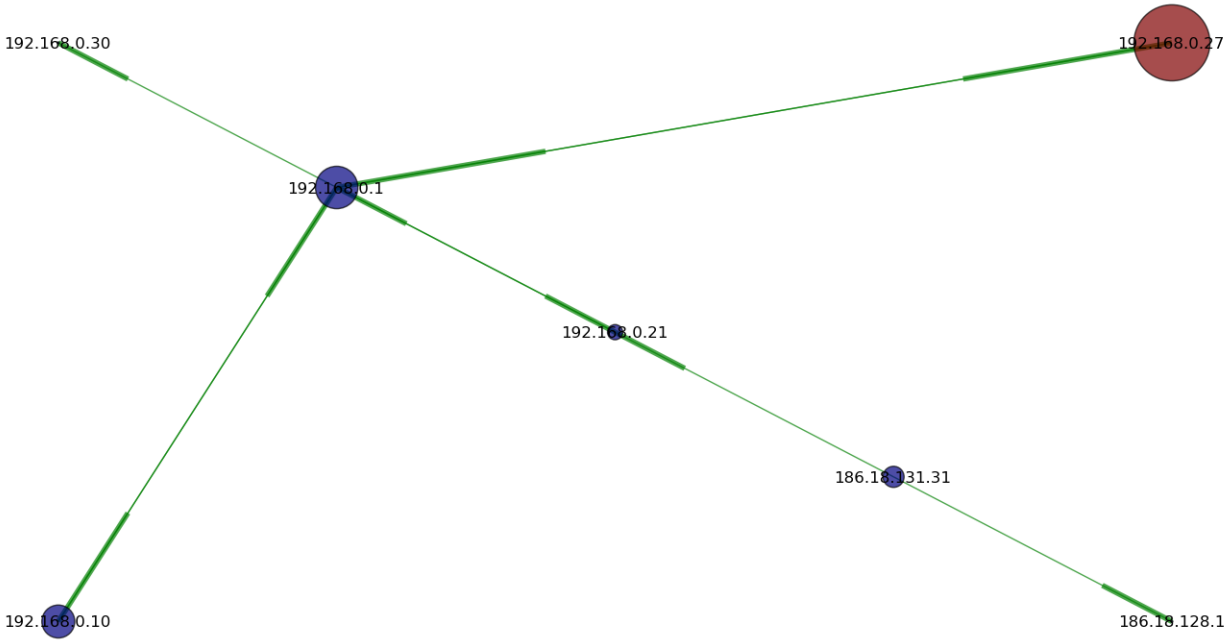

Figura 6: Red WiFi casa doméstica 2

3.3. Red Ethernet Empresa 1

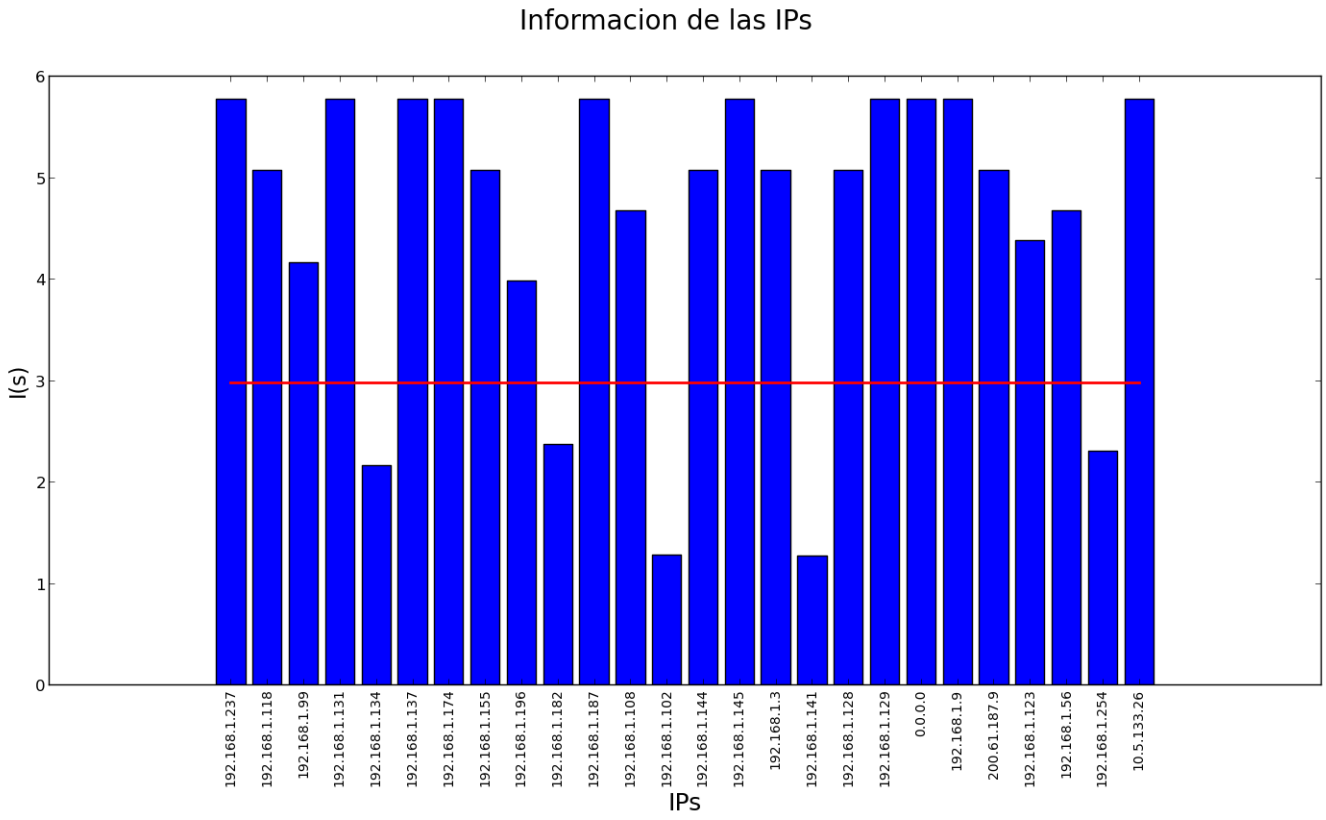

Figura 7: Fuente de información: IPs que envían

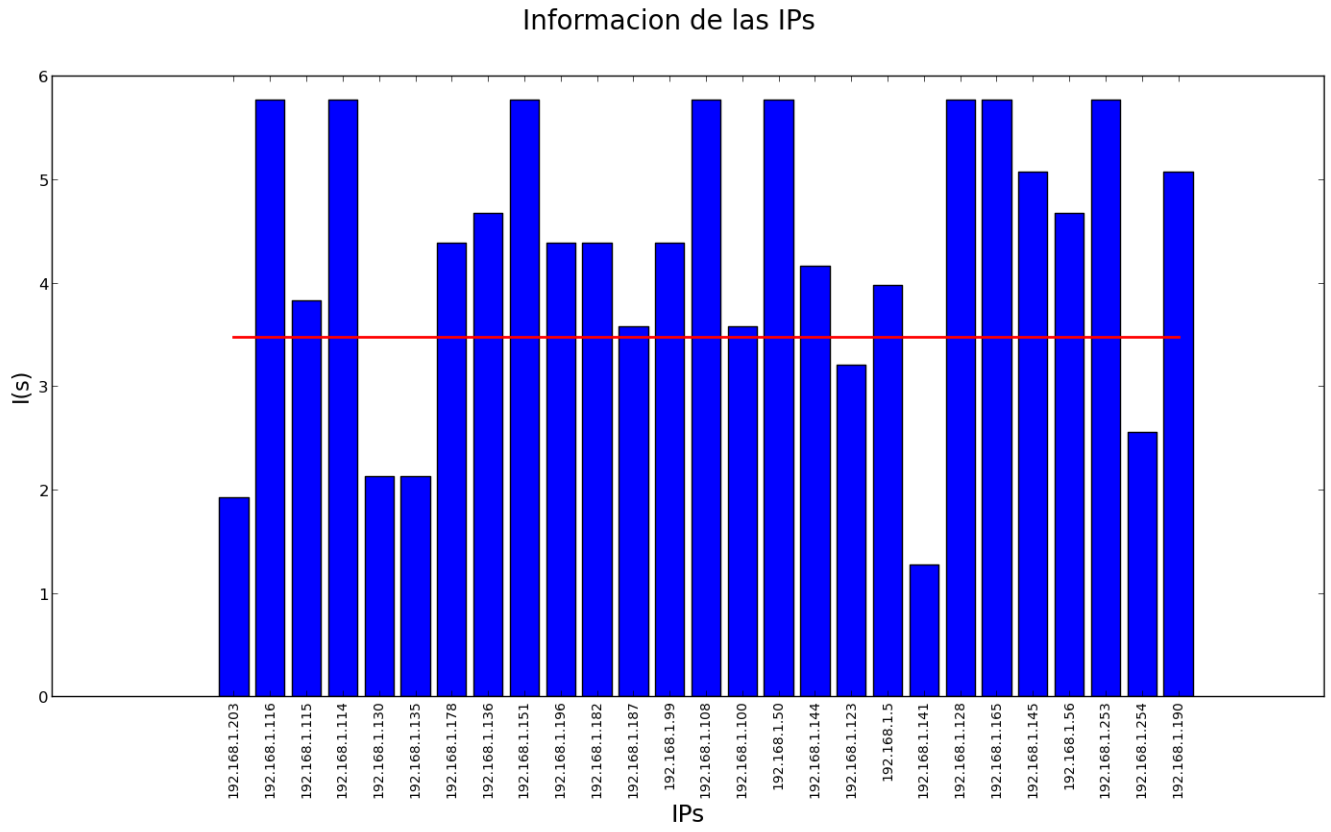

Figura 8: Fuente de información: IPs que reciben

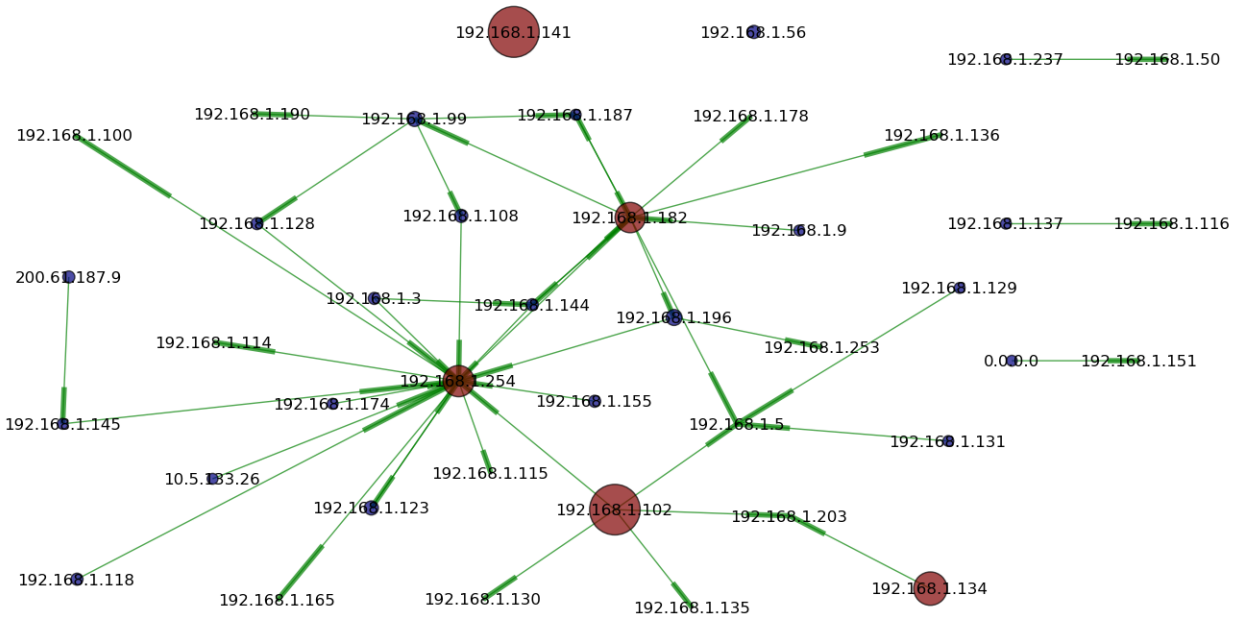

Figura 9: Red Ethernet de Recursiva

3.4. Red Ethernet Empresa 2

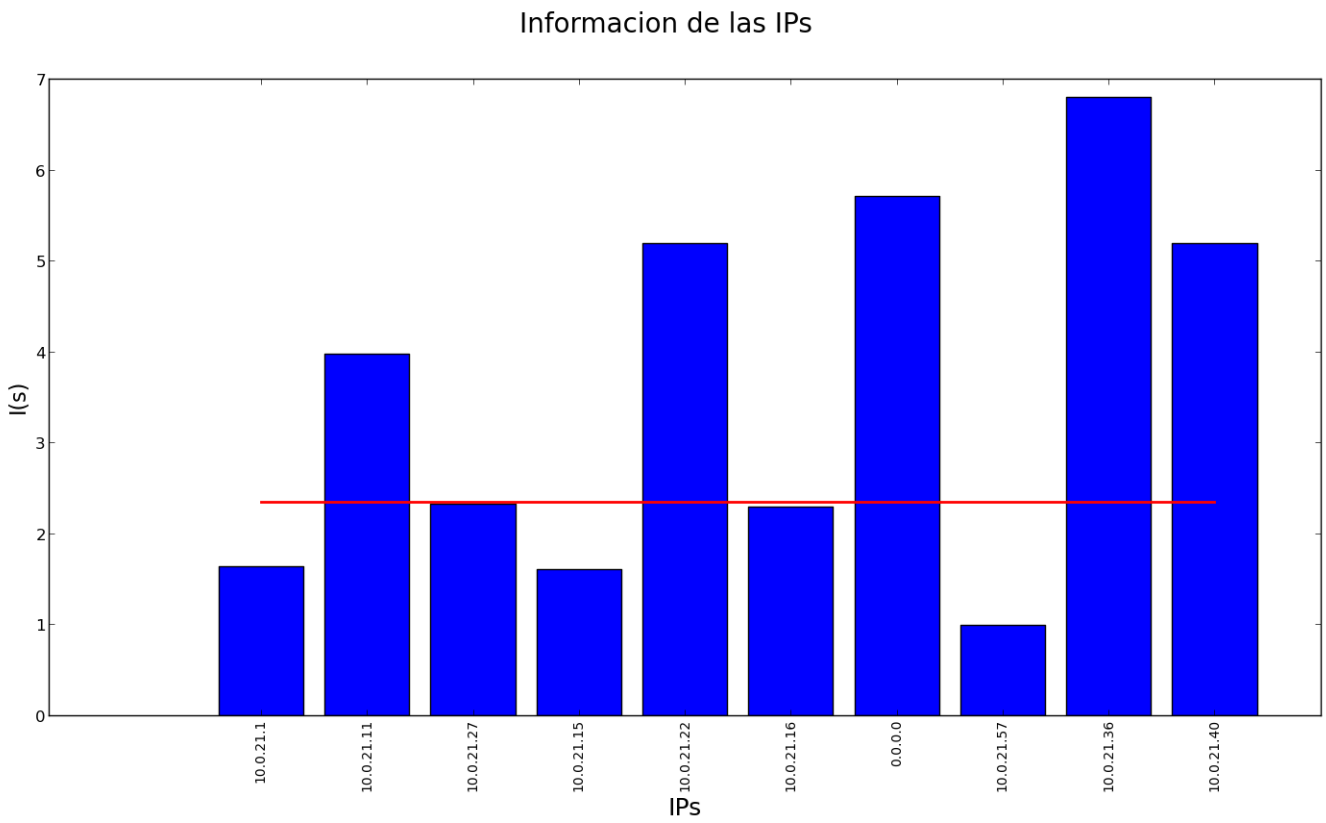

Figura 10: Fuente de información: IPs que envían

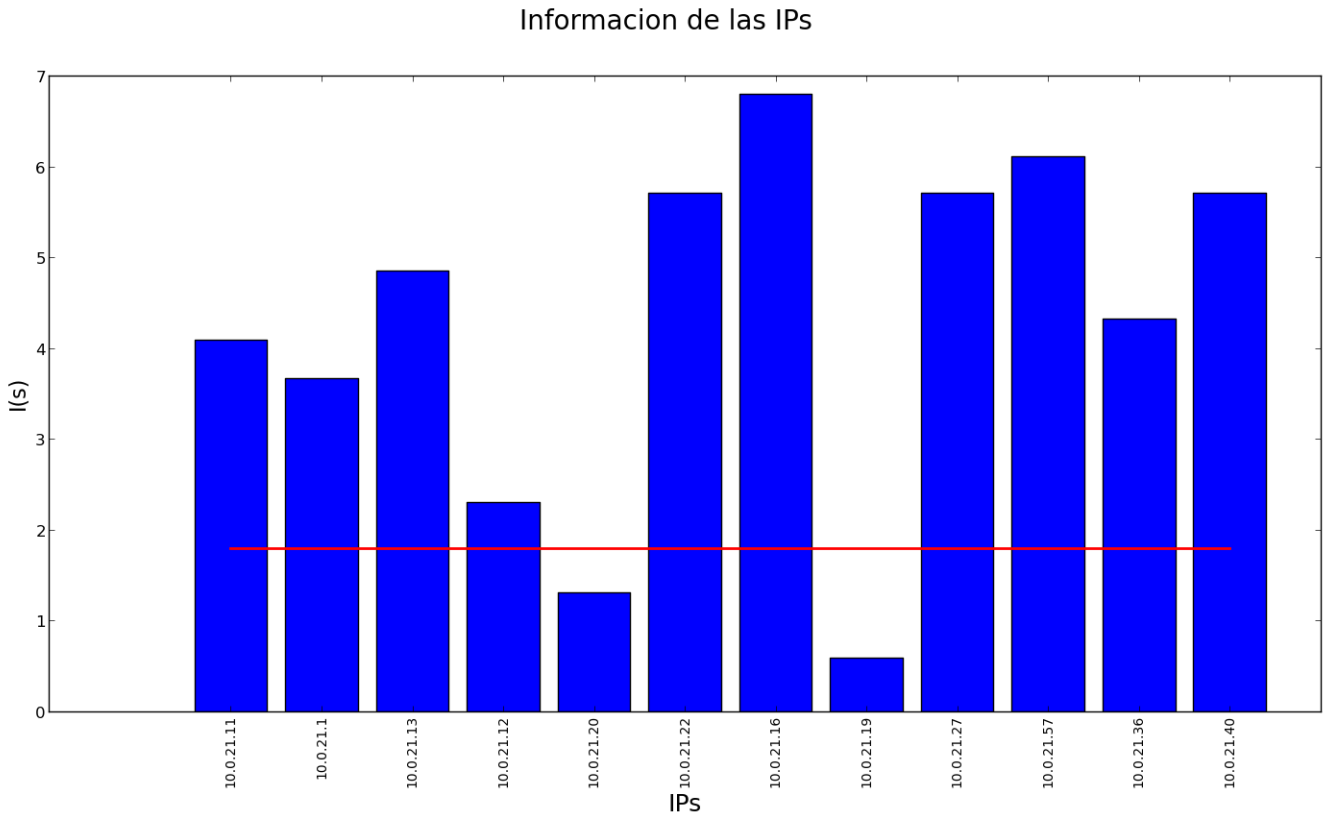

Figura 11: Fuente de información: IPs que reciben

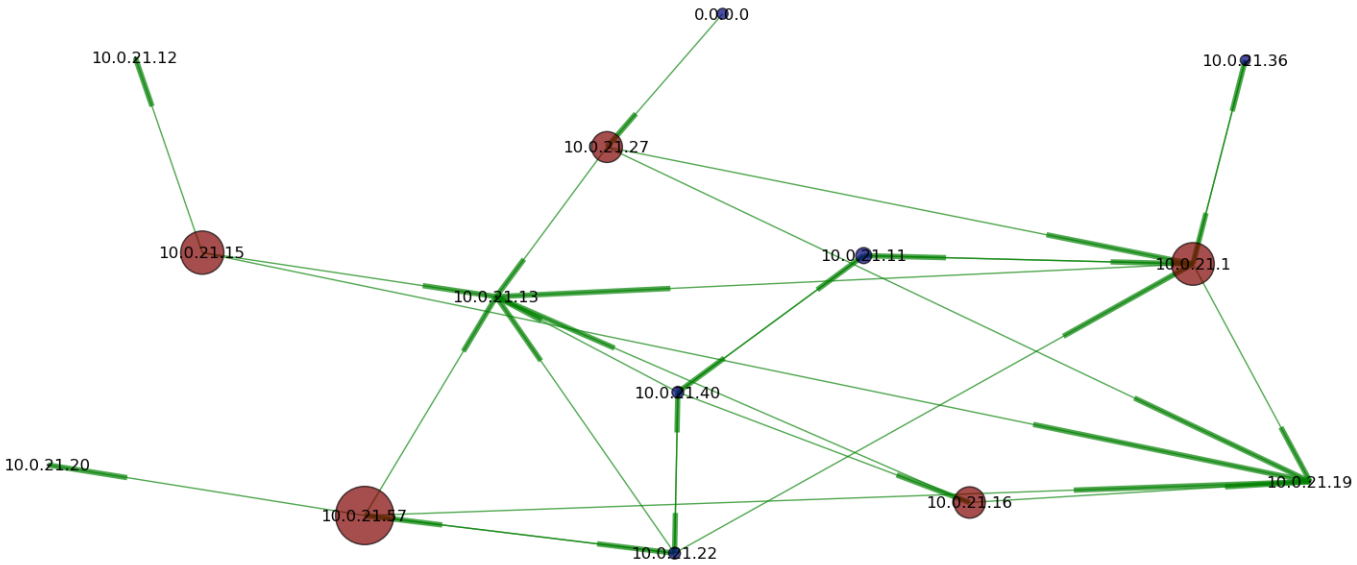

Figura 12: Red Ethernet de ORSNA

3.5. Red WiFi local comercial

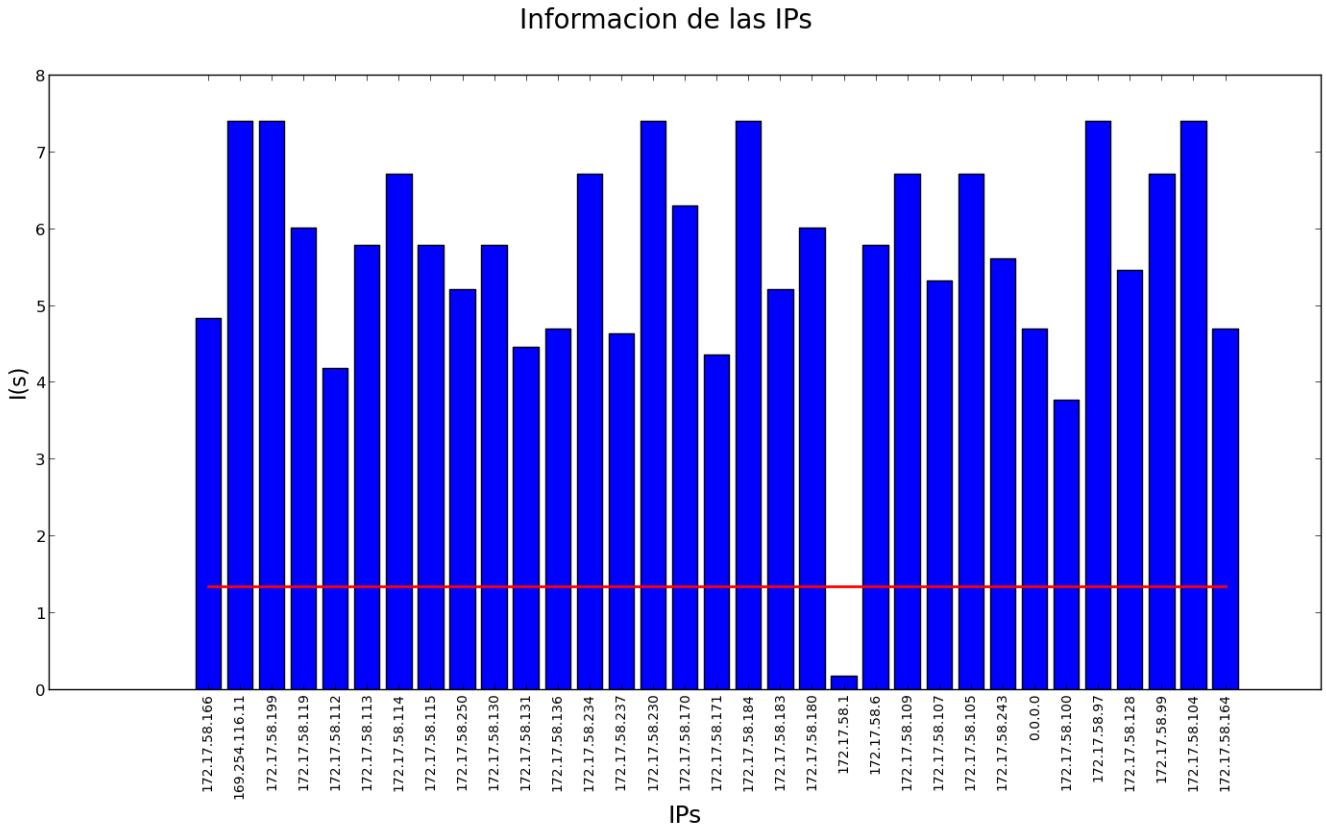

Figura 13: Fuente de información: IPs que envían

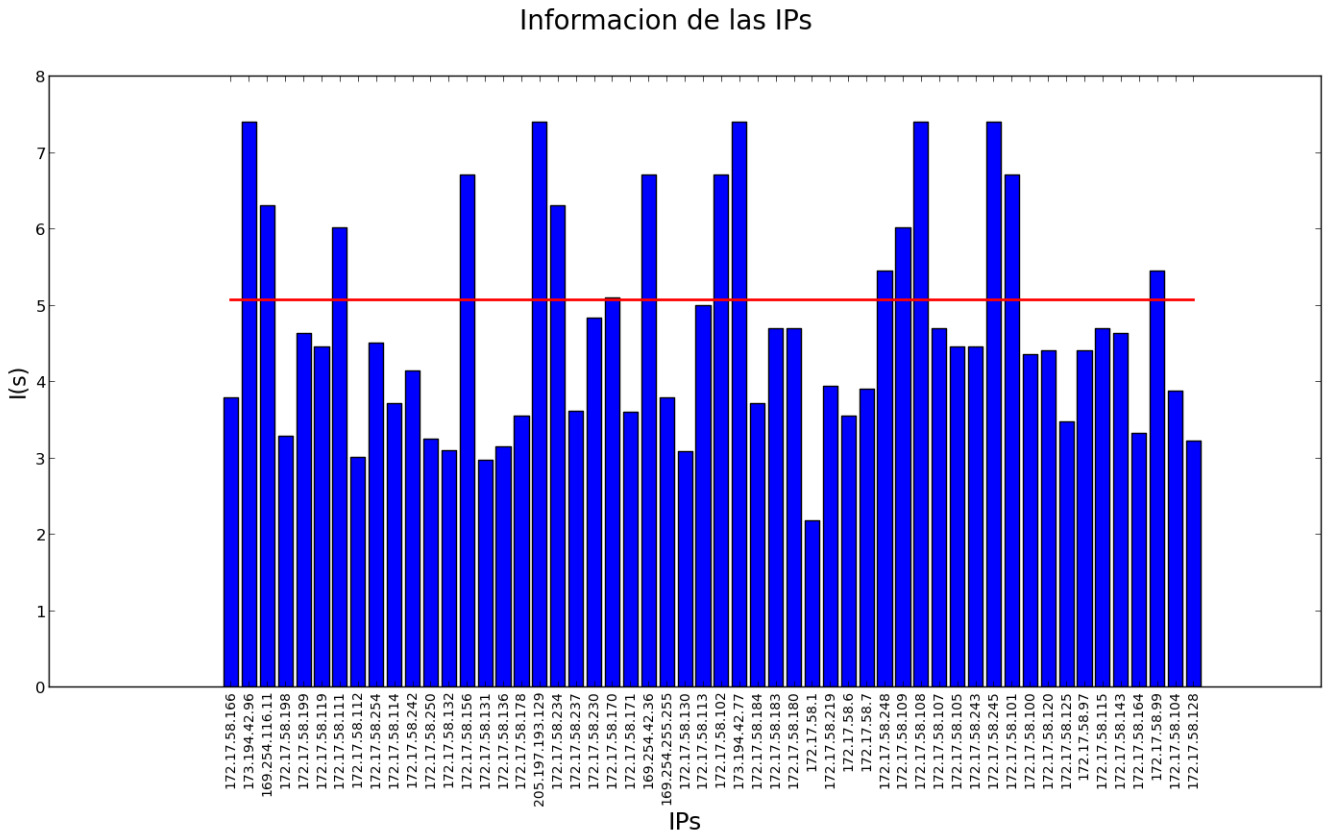

Figura 14: Fuente de información: IPs que reciben

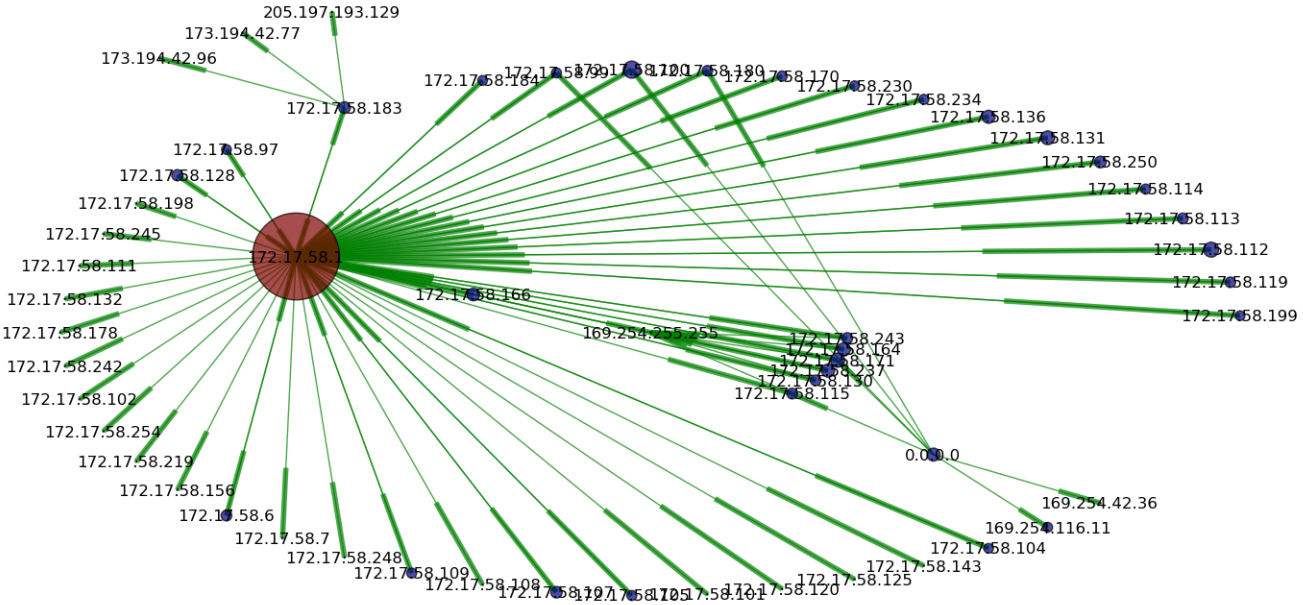

Figura 15: Red WiFi de McDonalds

4. Conclusiones