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 de distintas redes inalámbricas aún cuando estos paquetes no estaban destinados a nuestro host. 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. Valiendonos 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. Y para ello nos basamos en

3. Gráficos y análisis

3.1. Red WiFi casa particular 1

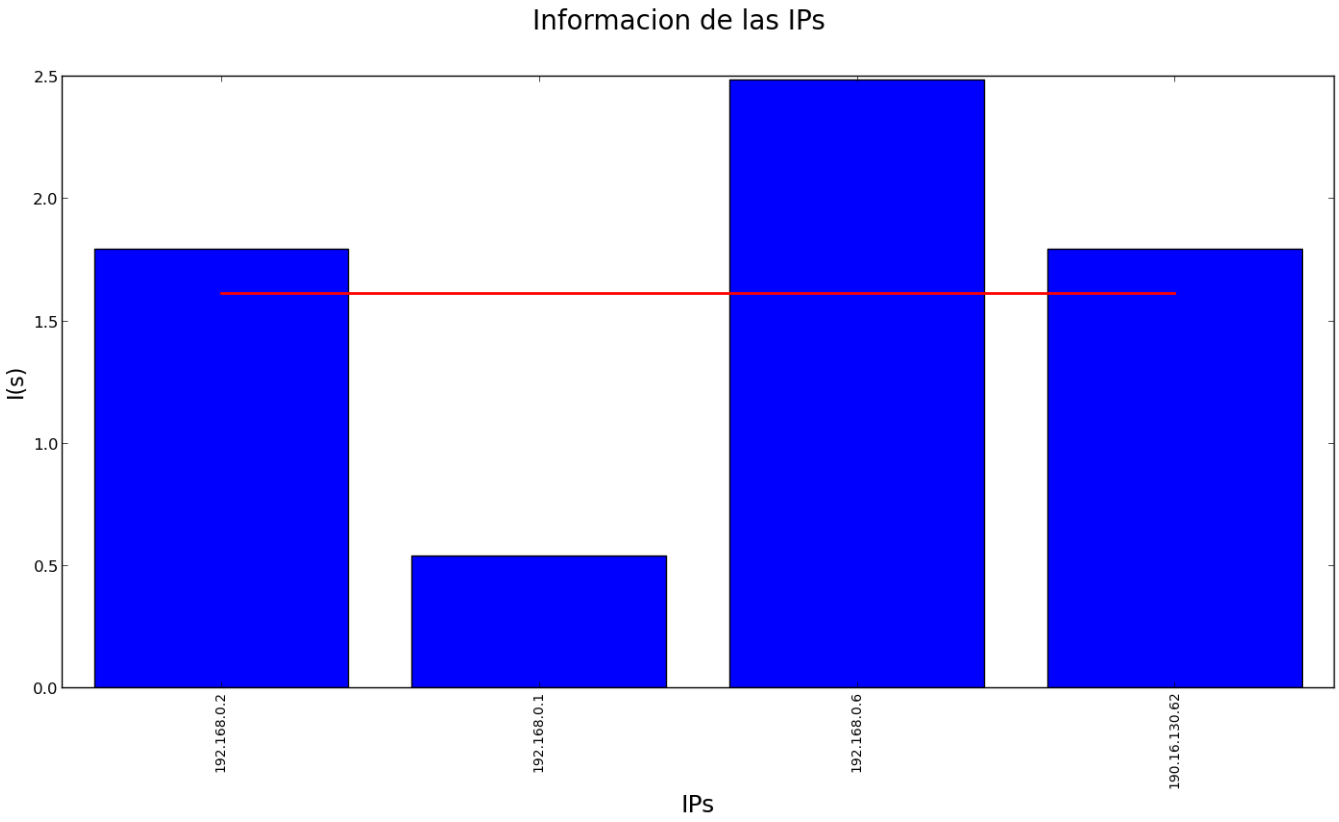

Figura 1: Fuente de información: IPs que envían

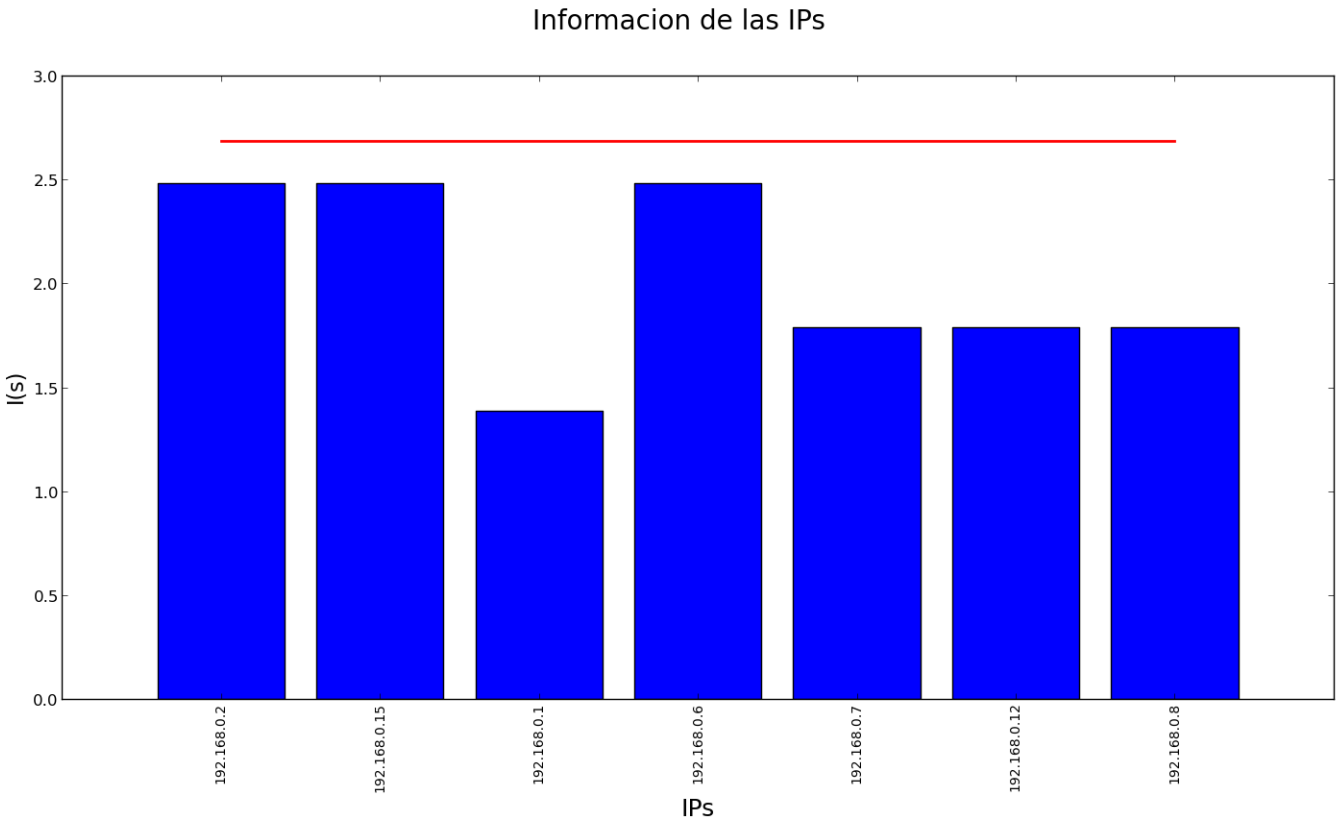

Figura 2: Fuente de información: IPs que reciben

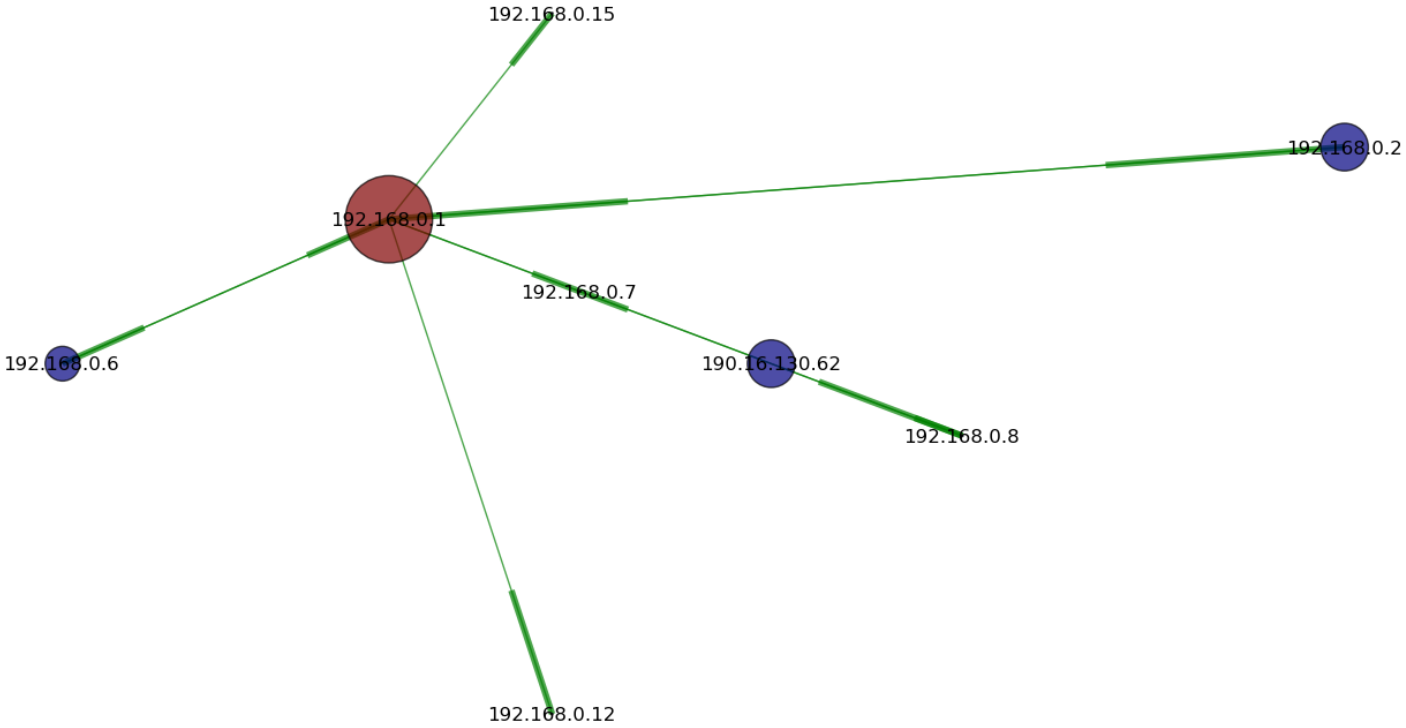

Figura 3: Red WiFi casa doméstica 1

3.2. Red WiFi casa particular 2

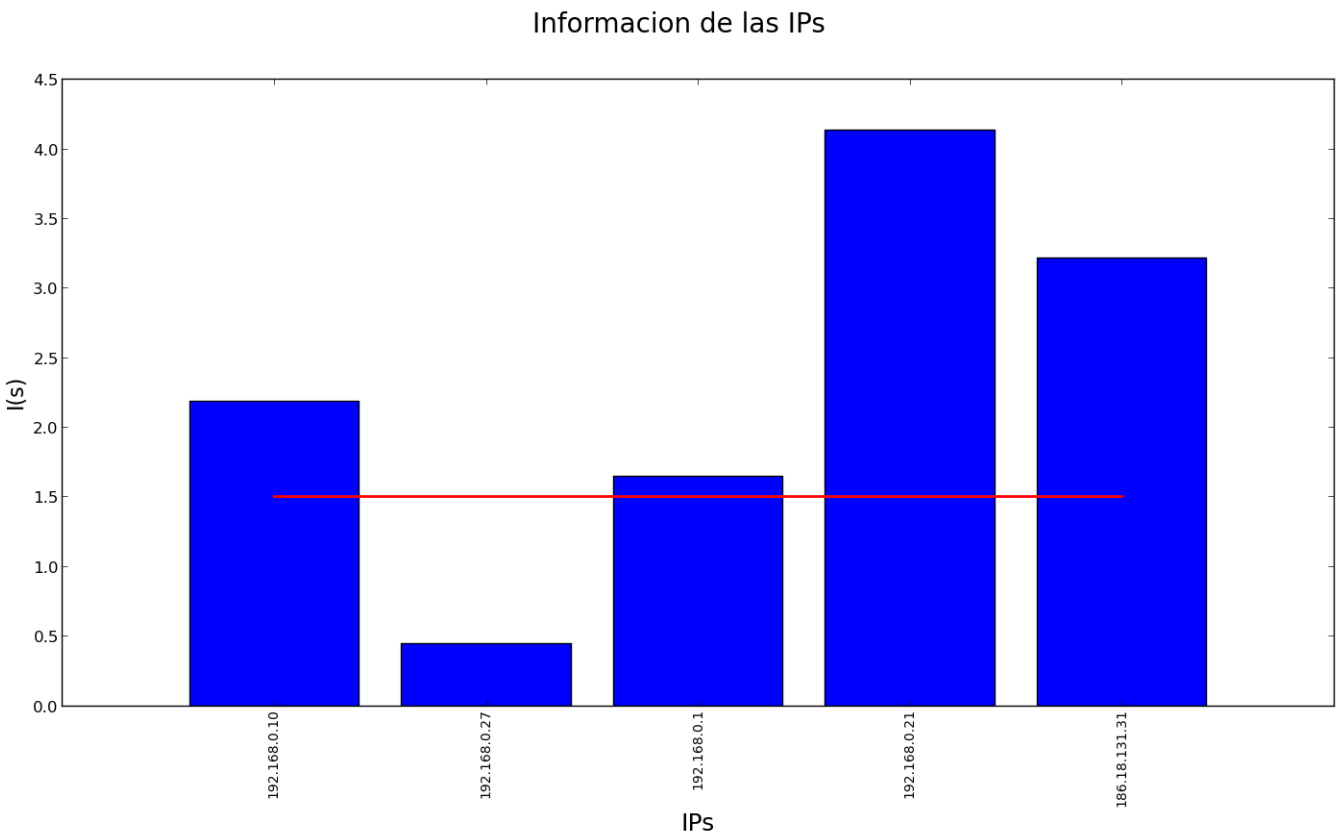

Figura 4: Fuente de información: IPs que envían

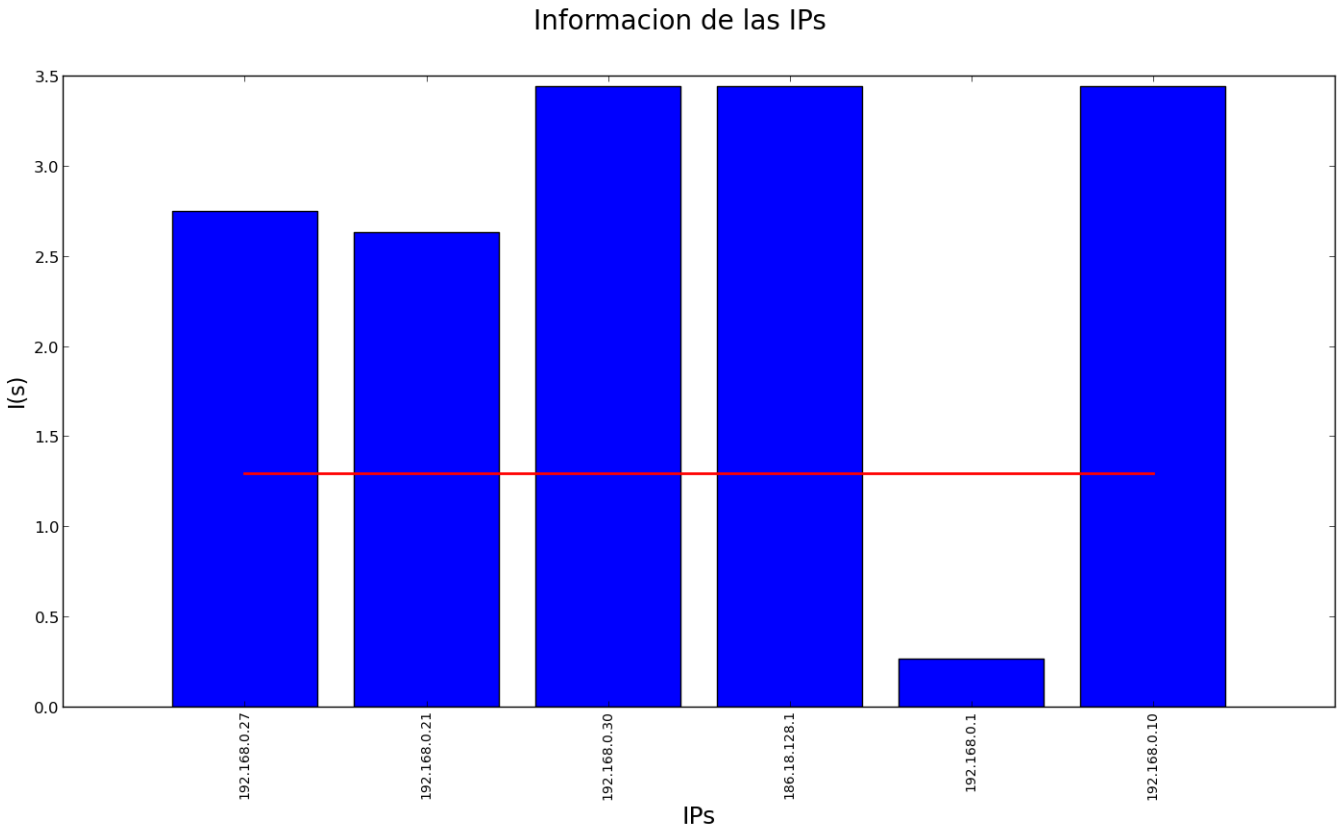

Figura 5: Fuente de información: IPs que reciben

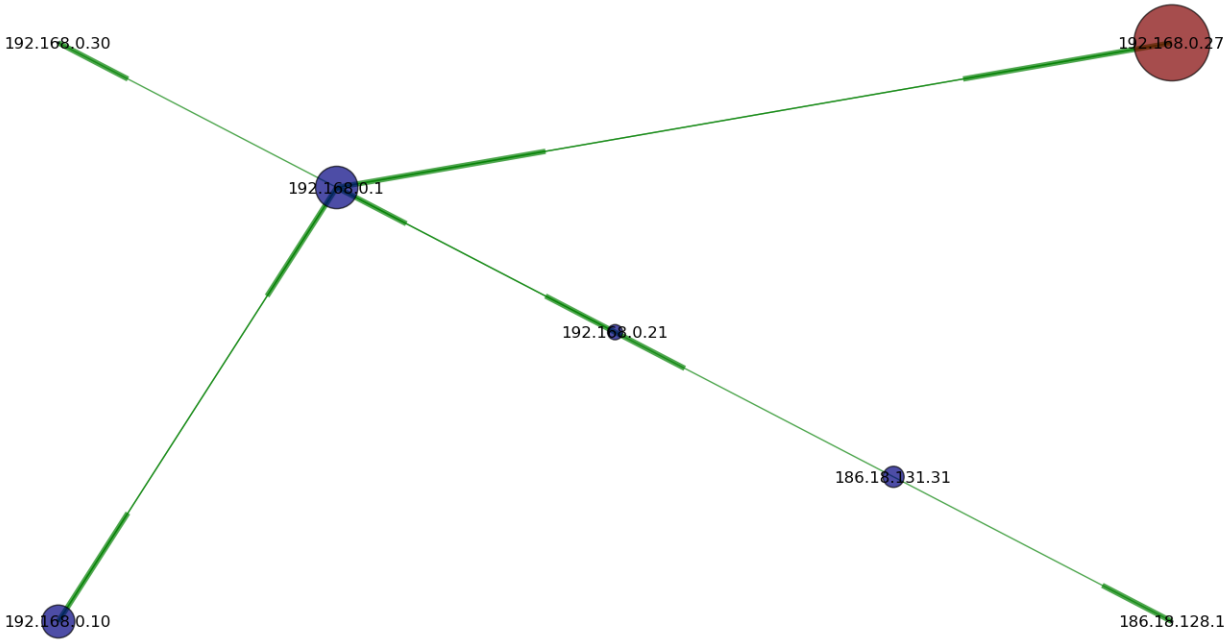

Figura 6: Red WiFi casa doméstica 2

3.3. Red Ethernet Empresa 1

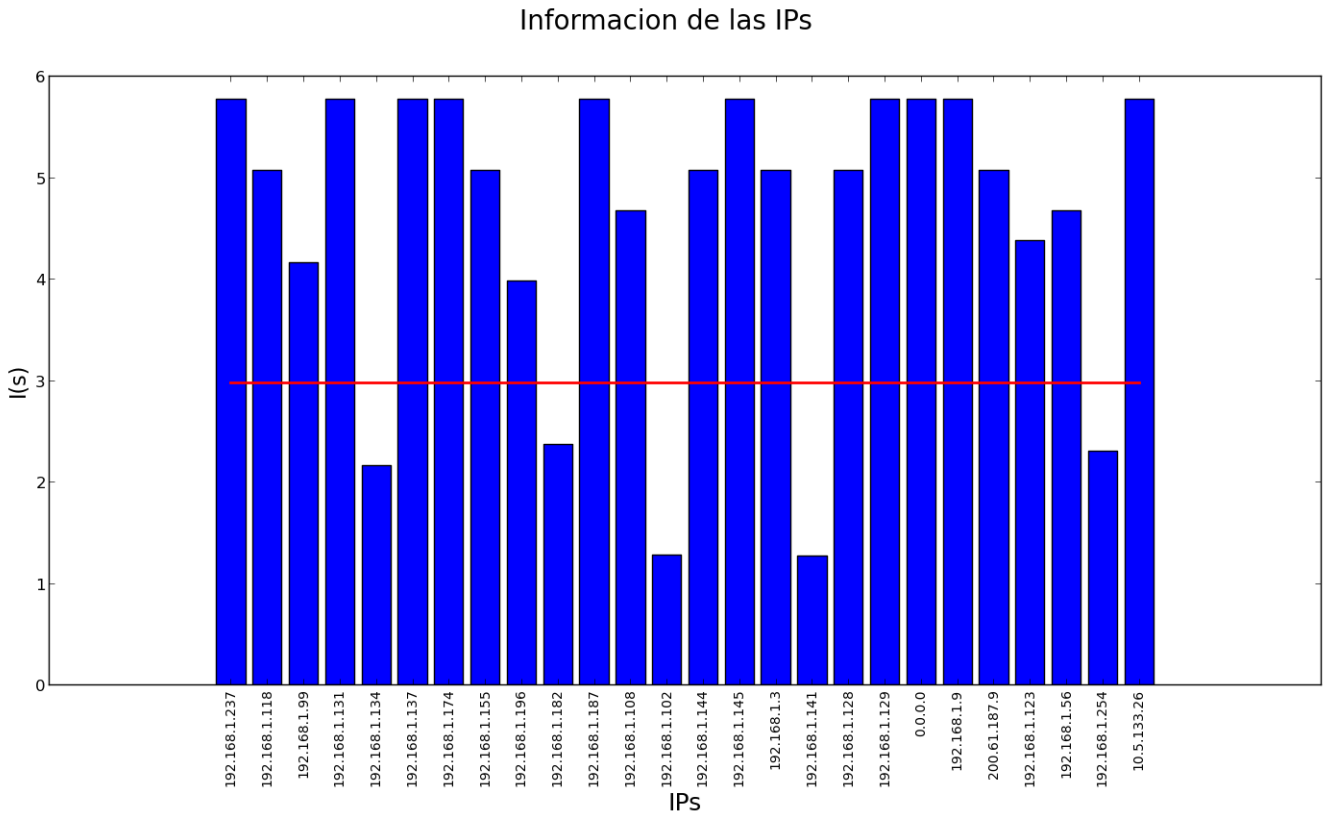

Figura 7: Fuente de información: IPs que envían

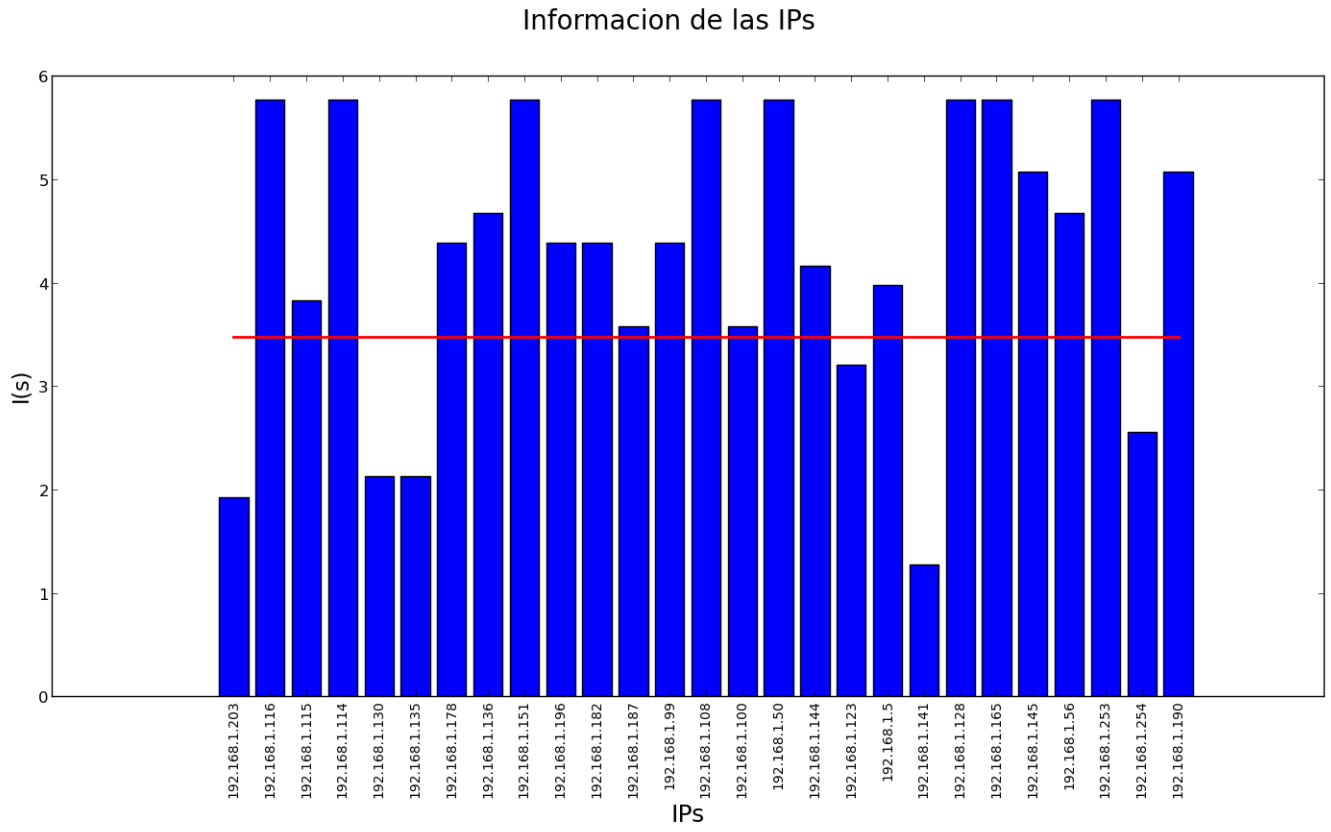

Figura 8: Fuente de información: IPs que reciben

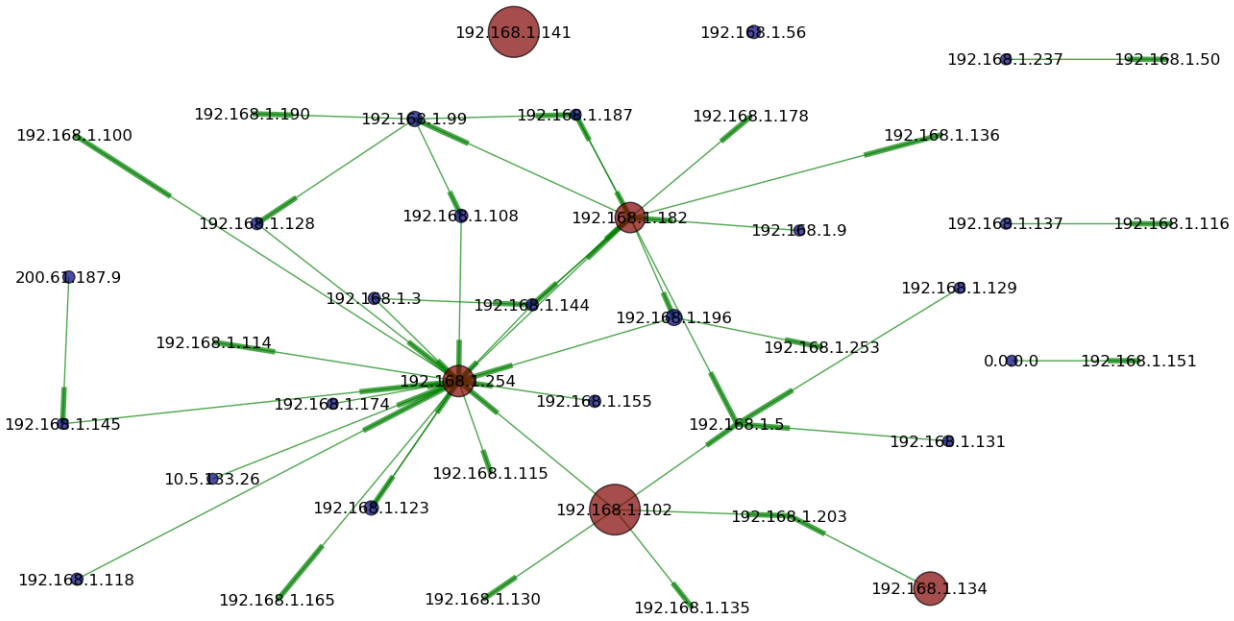

Figura 9: Red Ethernet de Recursiva

3.4. Red Ethernet Empresa 2

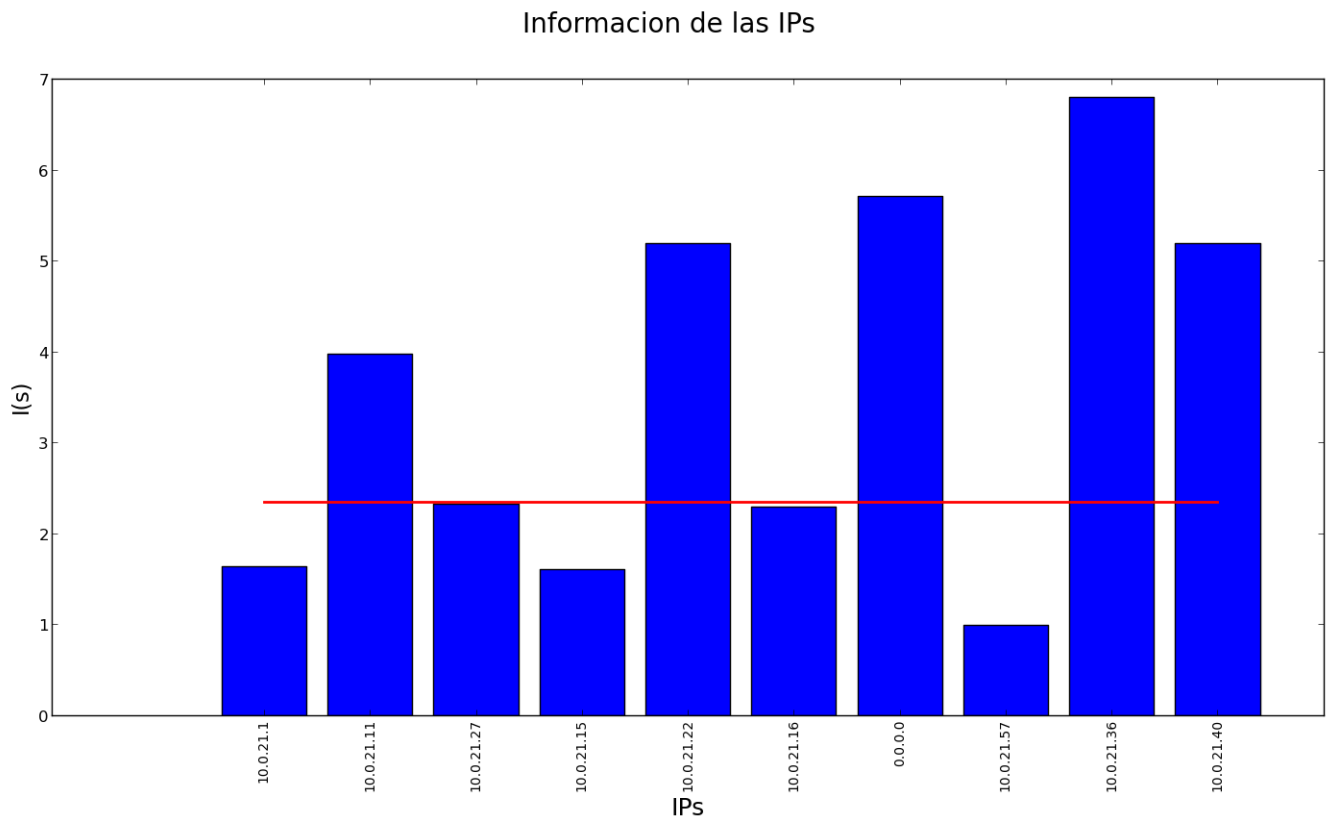

Figura 10: Fuente de información: IPs que envían

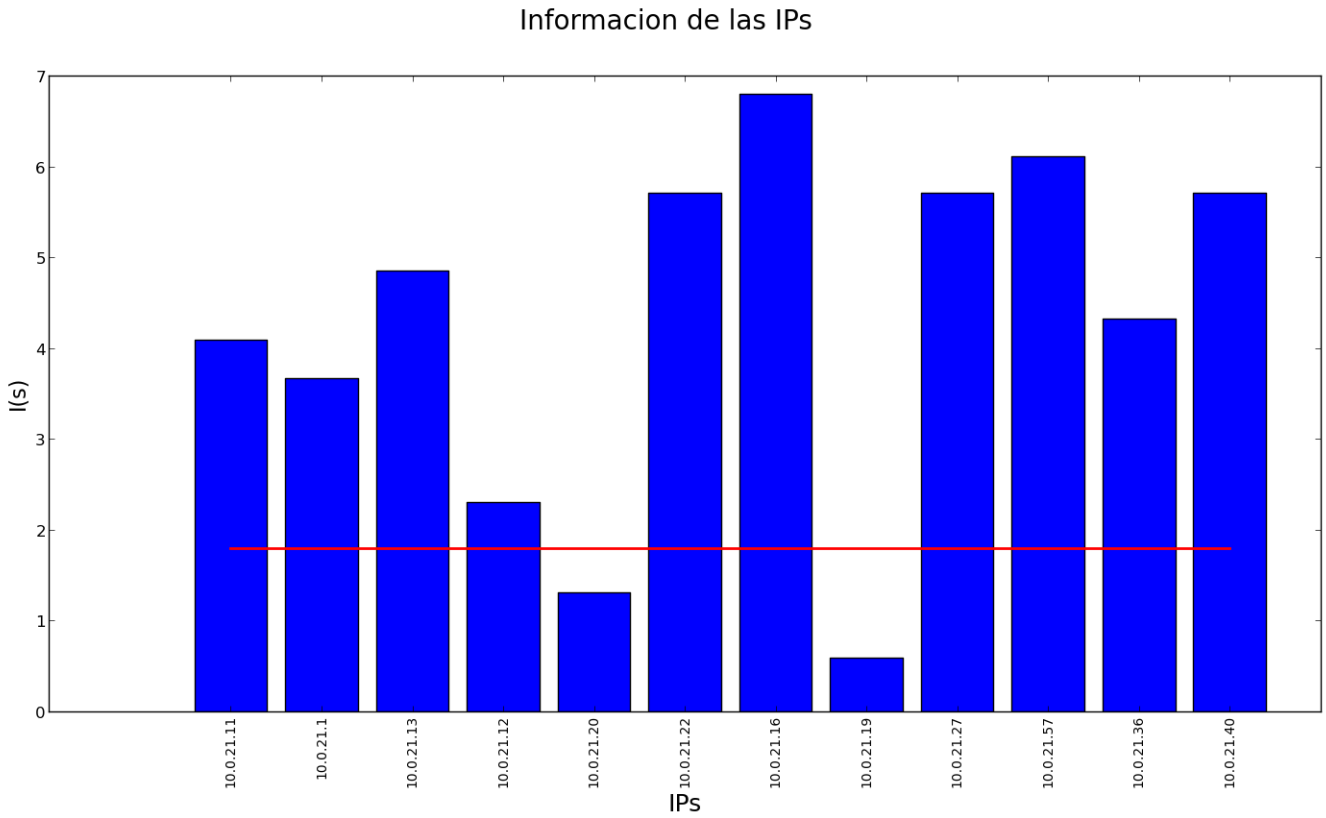

Figura 11: Fuente de información: IPs que reciben

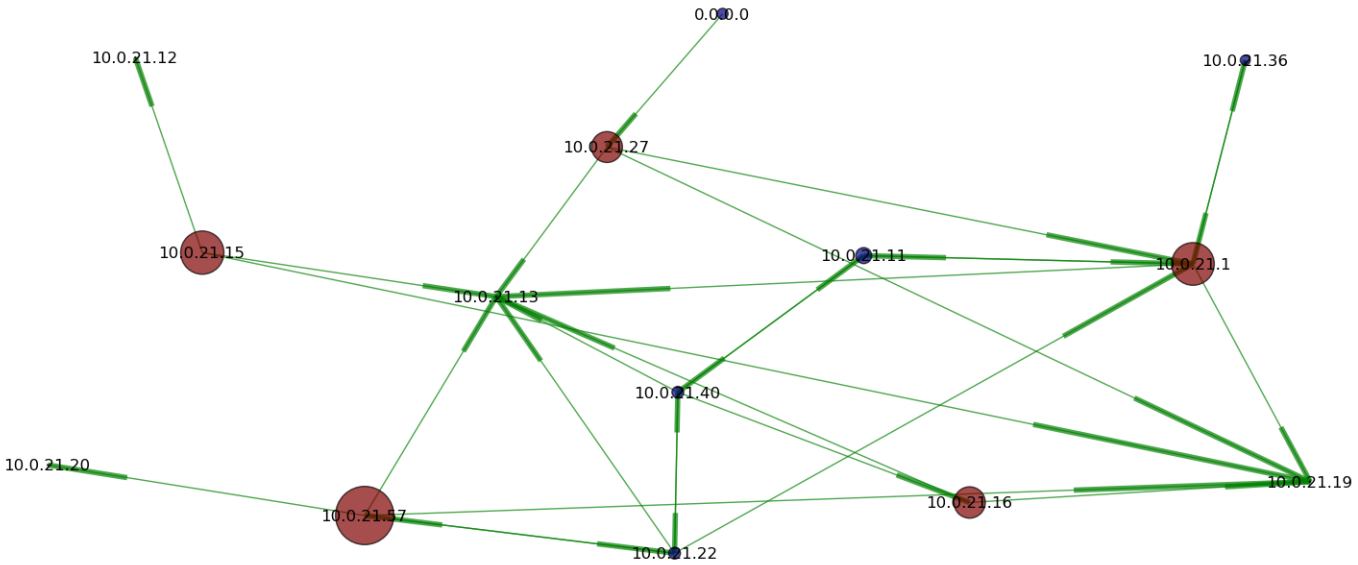

Figura 12: Red Ethernet de ORSNA

3.5. Red WiFi local comercial

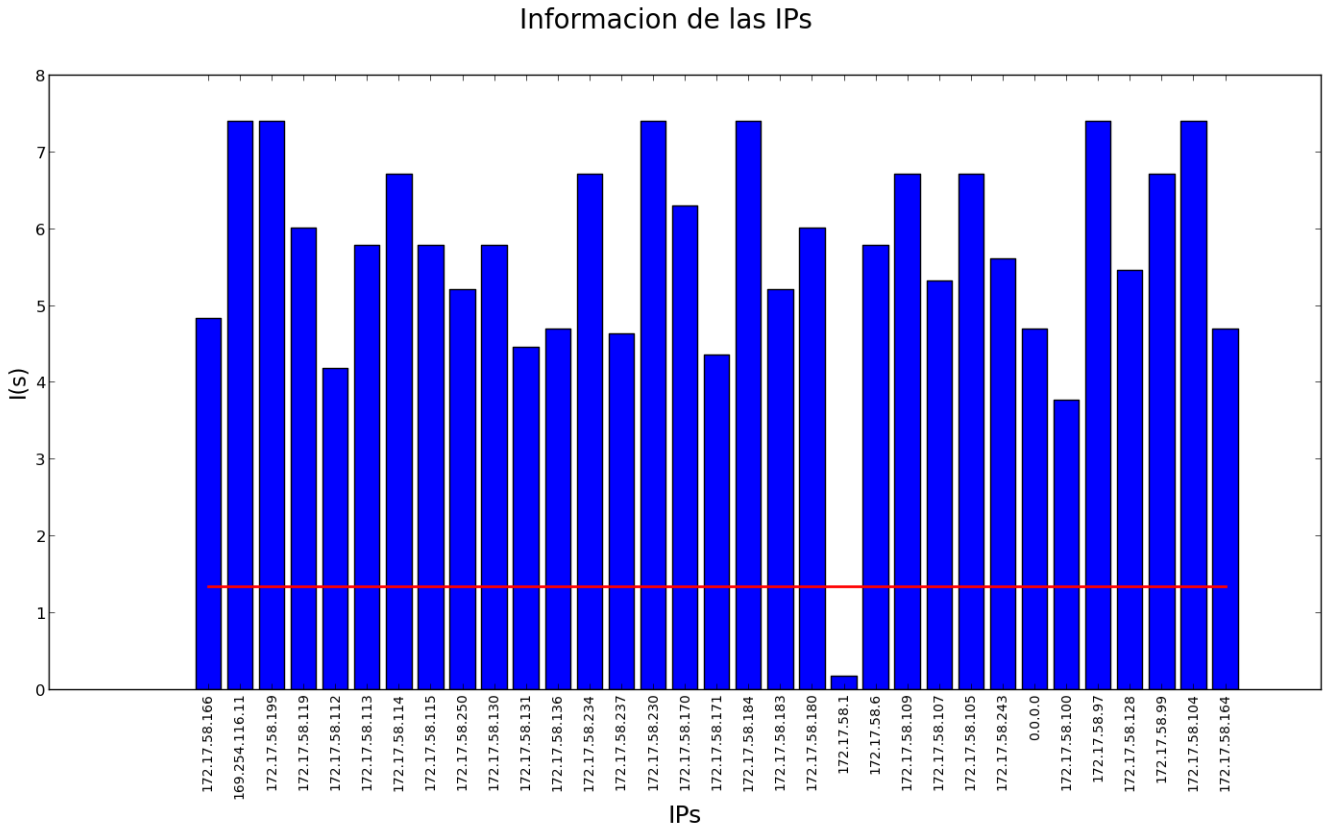

Figura 13: Fuente de información: IPs que envían

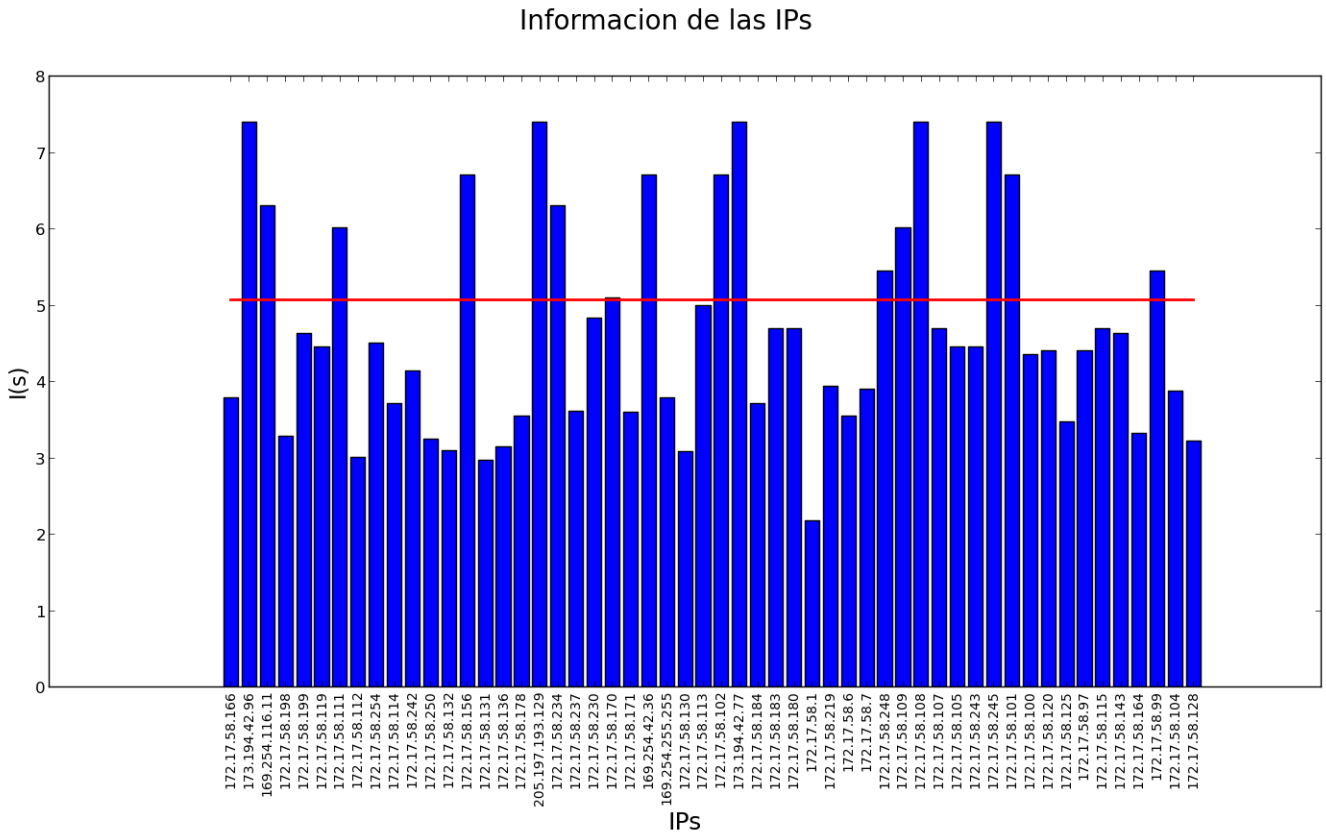

Figura 14: Fuente de información: IPs que reciben

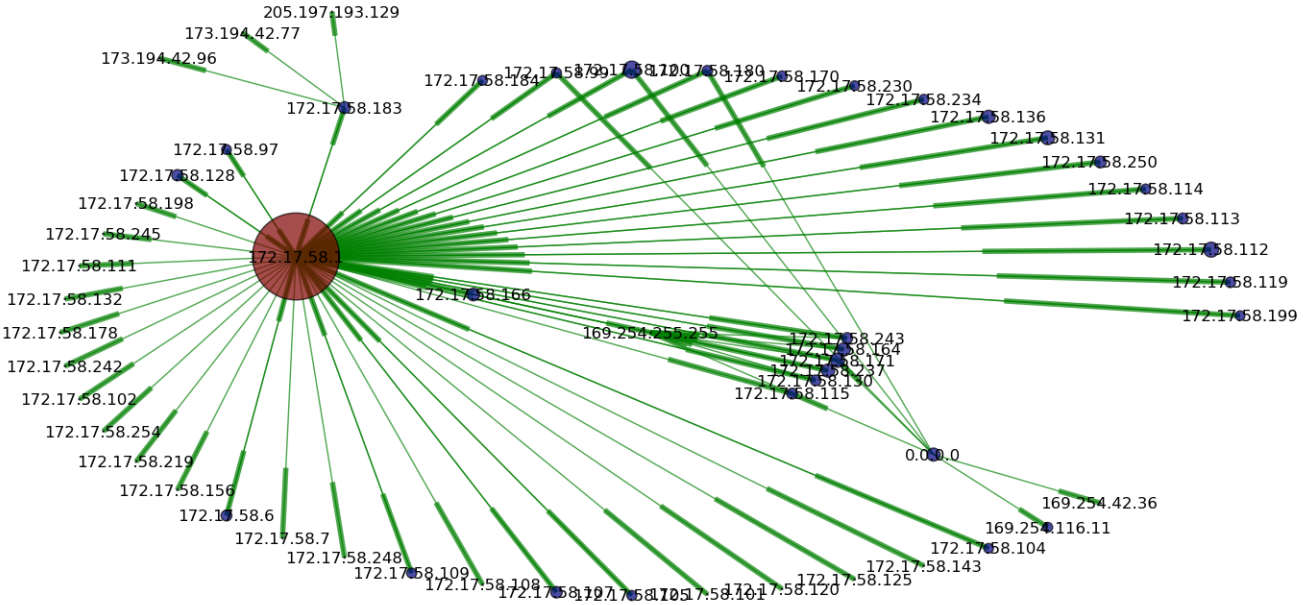

Figura 15: Red WiFi de McDonalds

4. Conclusiones