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

Trabajo Práctico 1

Teoría de las Comunicaciones

Primer Cuatrimestre de 2014

Apellido y Nombre	LU	E-mail
Delgado, Alejandro N.	601/11	nahueldelgado@gmail.com
Lovisolo, Leandro	645/11	leandro@leandro.me
Petaccio, Lautaro José	443/11	lausuper@gmail.com

Índice

1. Introducción téorica

En este trabajo realizamos un análisis de redes mediante la captura de paquetes ARP.

Address Resolution Protocol (ARP) es un protocolo usado frecuentemente por las redes locales para conectar las capas 3 (capa de red) y 2 (capa de enlace) mediante la conversión o identificación de IP's v4 con direcciones físicas MAC's.

Existen dos tipos de paquetes posibles en el protocolo: paquetes de petición y de respuesta.

- Los paquetes de petición (`who-has`) son enviados mayormente en forma de broadcast con el objetivo de poder localizar la dirección MAC a la cuál le pertenece una IP conocida.
- Los paquetes de respuesta (`is-at`) son enviados de manera uni-cast ya que se utilizan para responder a la máquina que realizó una petición con anterioridad.

La estructura de los paquetes ARP es simple, consiste principalmente de los siguientes campos:

Operación	Especifica la operación que el emisor está realizando, 1 para petición, 2 para responder
Dirección MAC del emisor	
Dirección IP del emisor	
Dirección MAC del receptor	Este campo se ignora en las respuestas
Dirección IP del receptor	

Ejemplo práctico de su utilización:

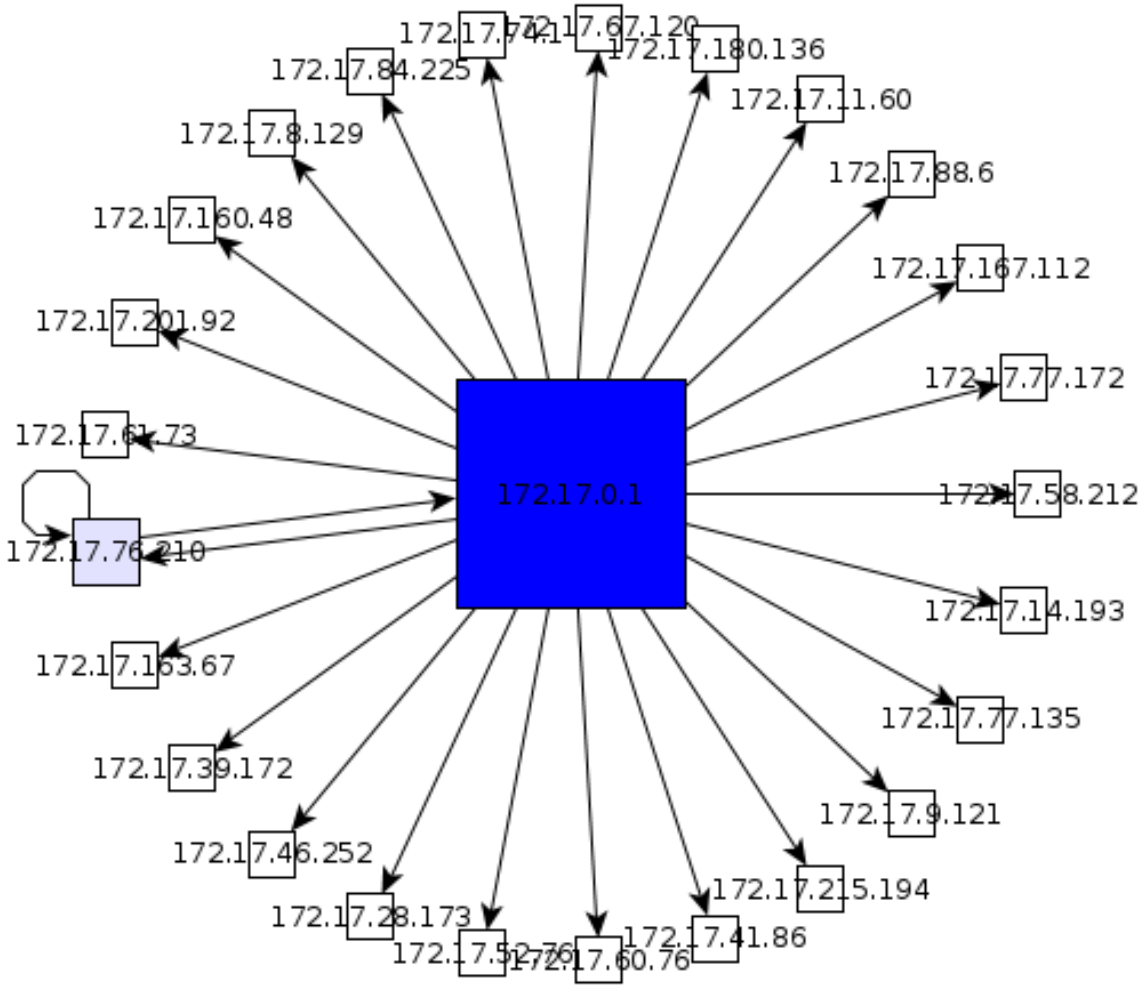
Una máquina en una red quiere mandarle un paquete de datos a otra máquina en la misma red. Para esto, la máquina emisora busca en su tabla local, la dirección MAC asociada a la dirección IP a la cuál quiere mandar el paquete. Si no la encuentra, realiza el broadcasts de la petición ARP, la cual llegará eventualmente, si se encuentra conectada, a la máquina destino. La máquina destino recibirá la petición y la responderá de manera uni-cast hacia la máquina que realizó la petición, poniendo en el paquete su dirección MAC para que la máquina destino de la respuesta pueda conocer la dirección MAC que necesitaba.

El análisis de la red consiste en reconocer su topología en base al nivel de información que proveen las diferentes IP's, como fuente y como destino, tomando a las IP's como símbolos y estimado su probabilidad de aparición con su frecuencia muestral.

2. Desarrollo

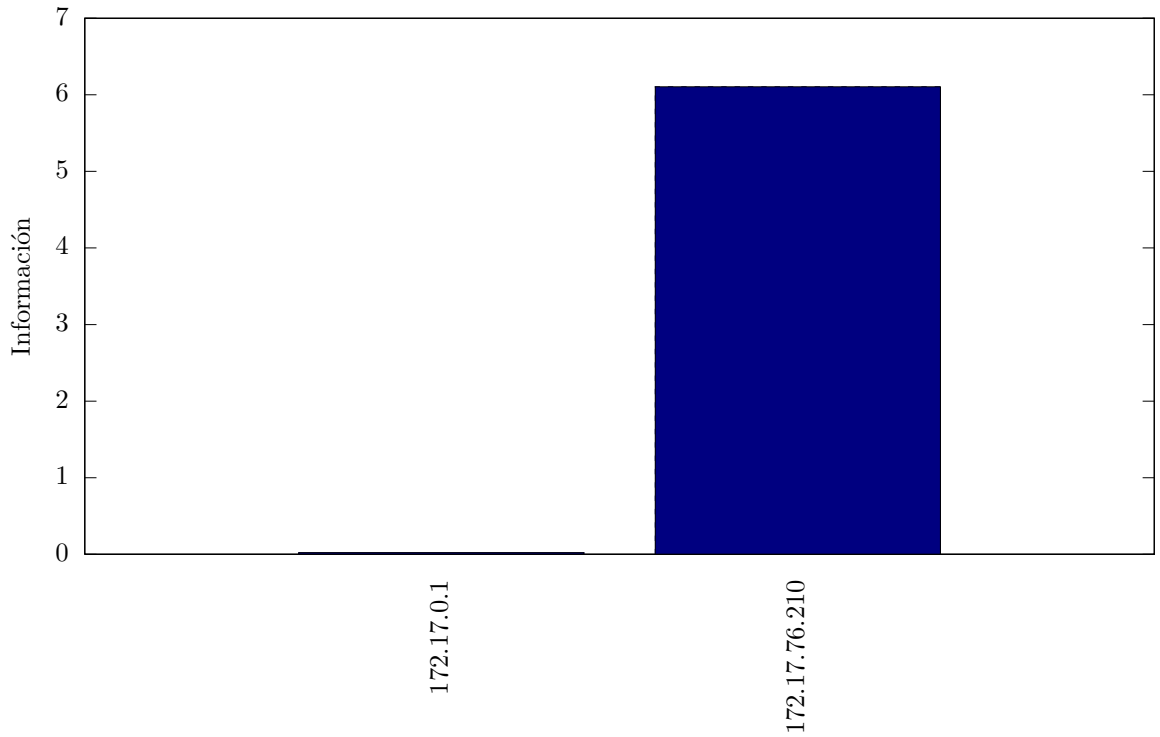
3. Resultados

3.1. Red *Alto Palermo*



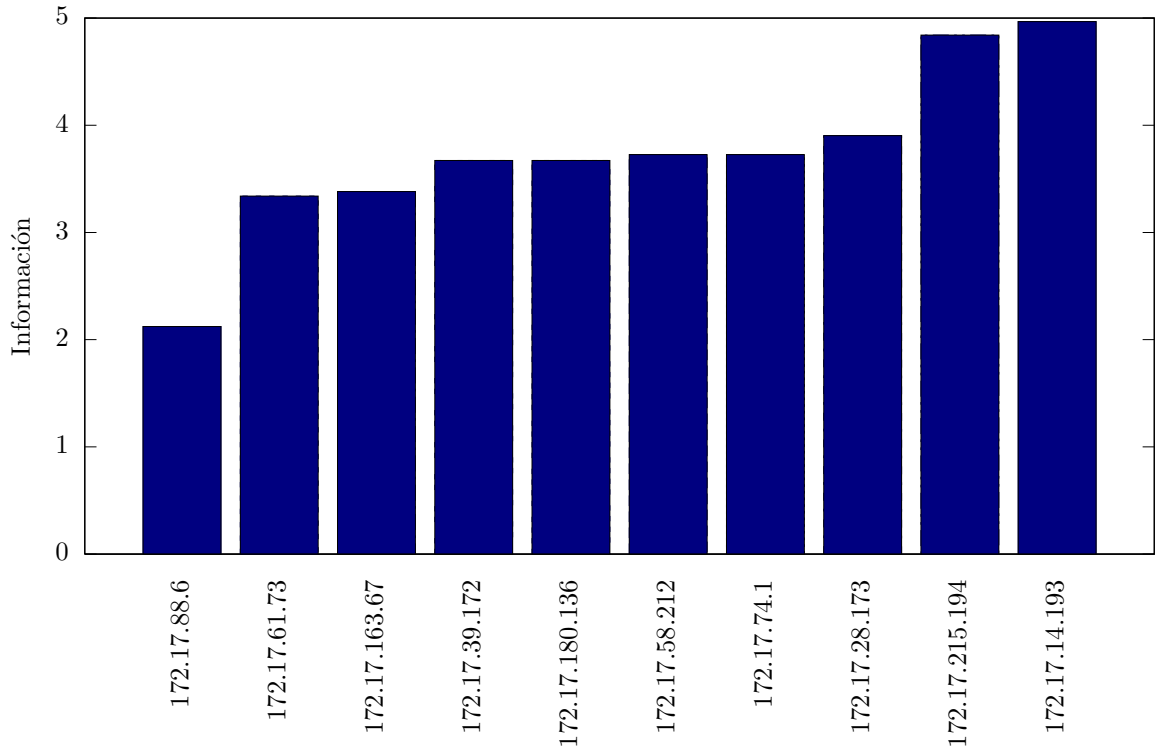
3.1.1. Información de los símbolos de la fuente de información S_{src}

Donde $S_{src} = \{$direcciones IP origen en paquetes ARP *who-has*$\}$.

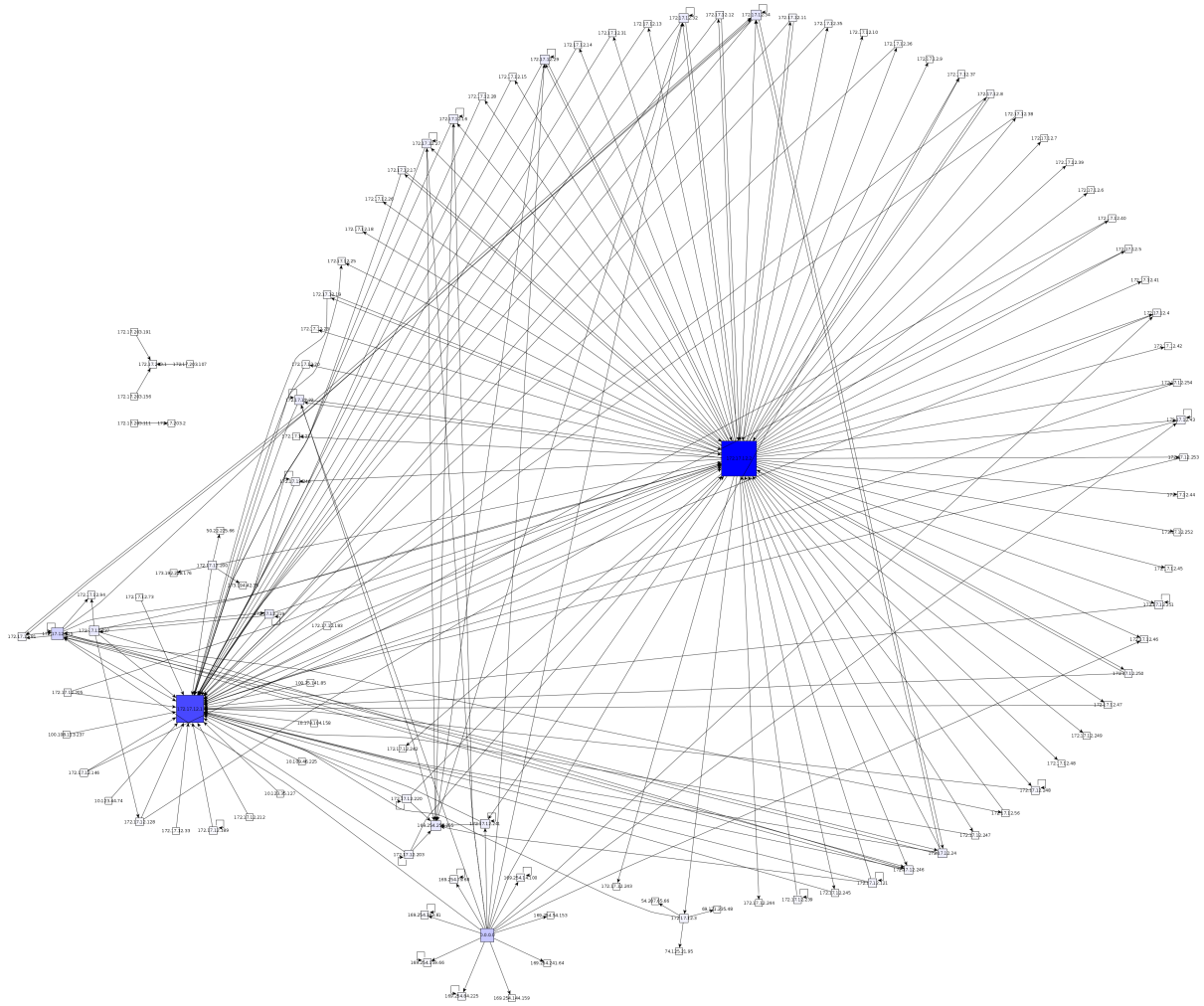


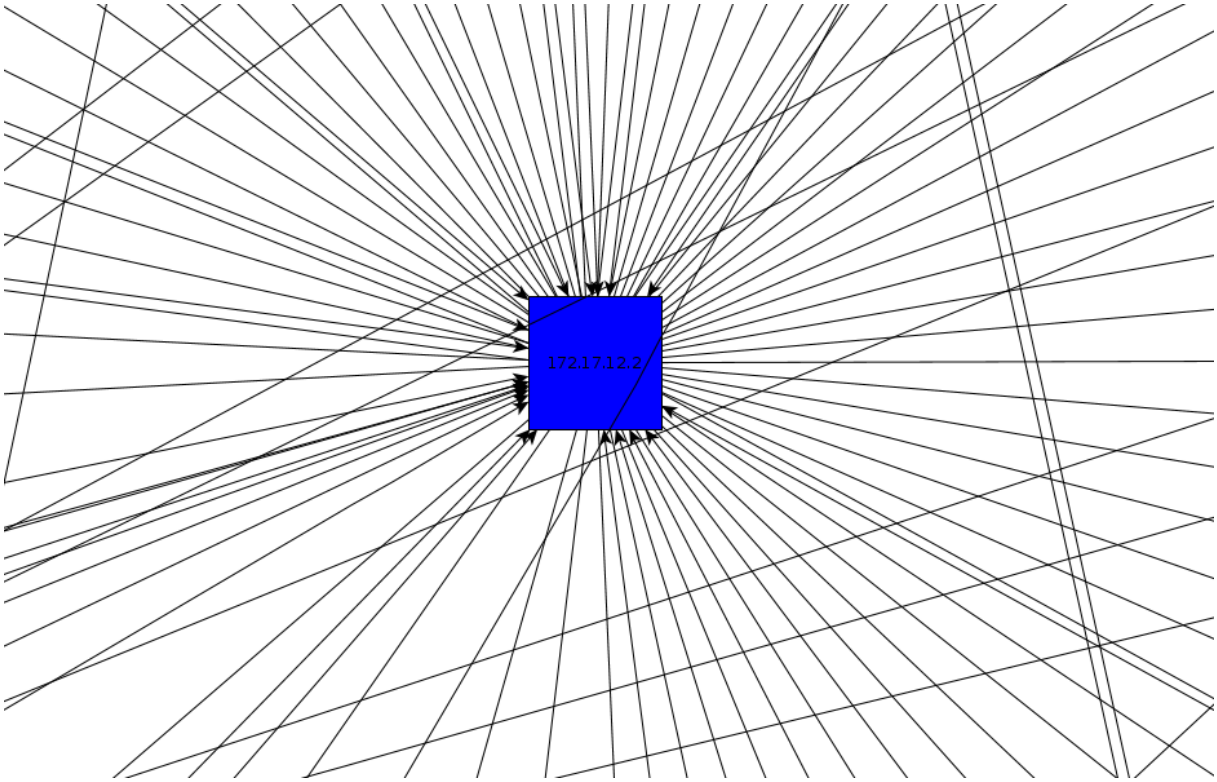
3.1.2. Información de los símbolos de la fuente de información S_{dst}

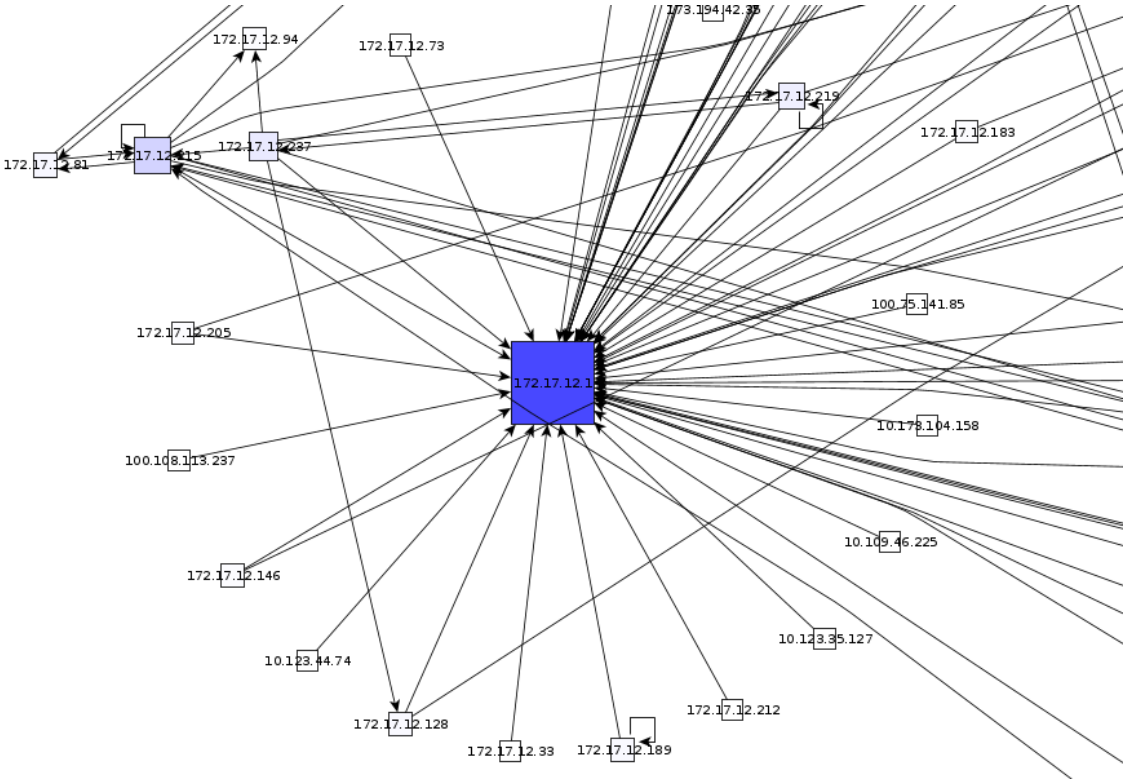
Donde $S_{dst} = \{$direcciones IP destino en paquetes ARP *who-has*$\}$.

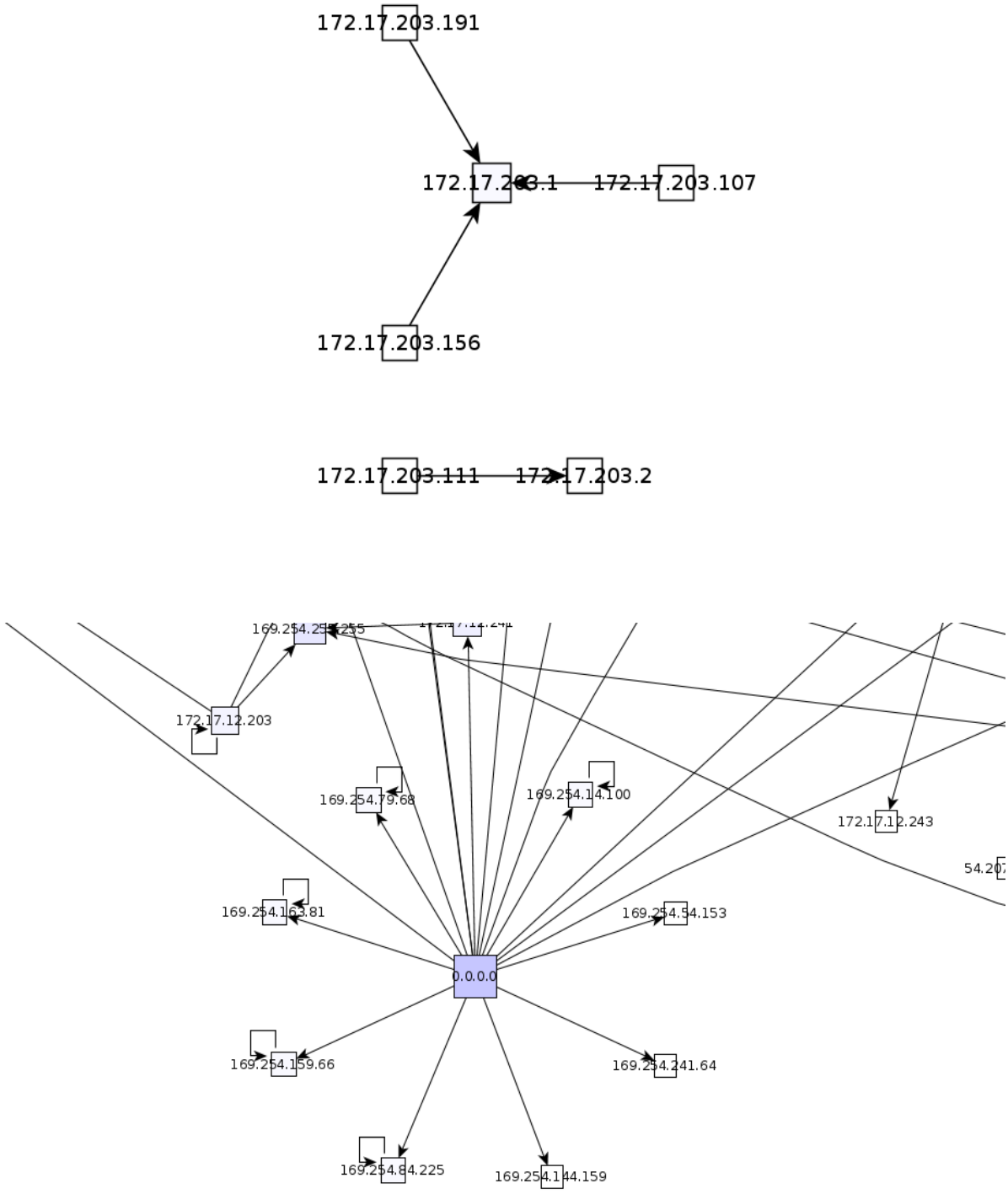


3.2. Red *McDonald's*



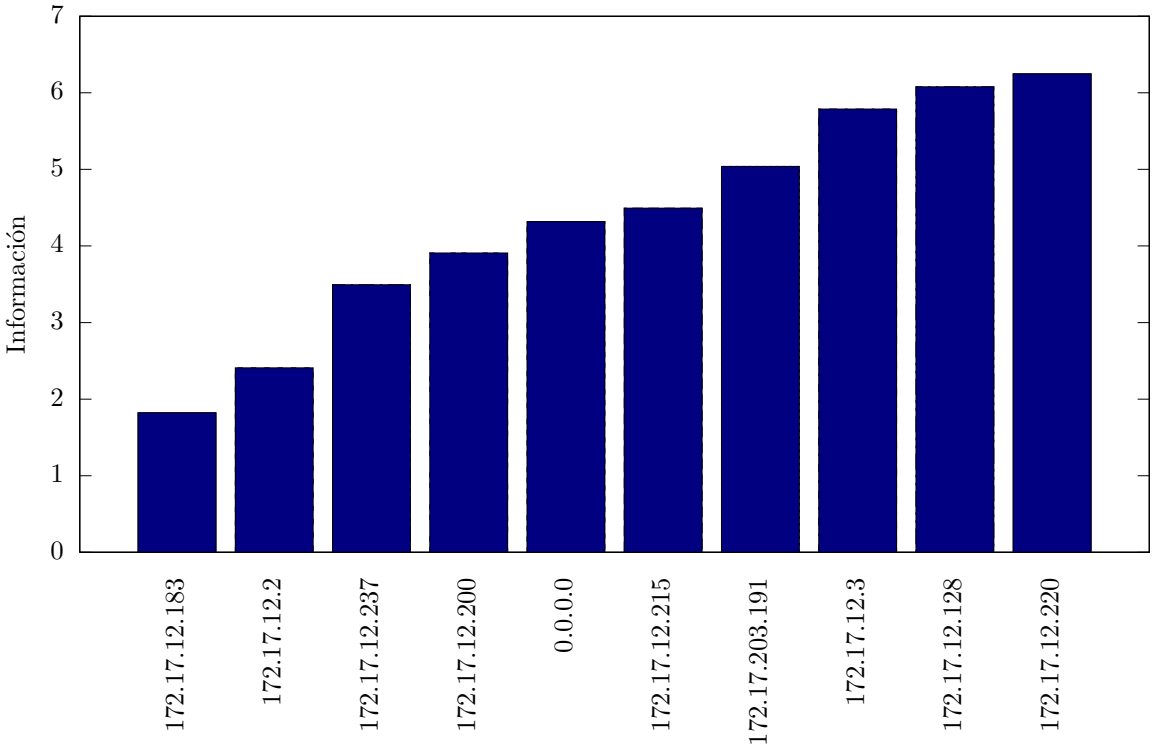

172.17.12.2


172.17.12.94
172.17.12.73
172.17.12.219
172.17.12.183
172.17.12.81
172.17.12.237
100.25.141.85
172.17.12.205
10.178.104.158
100.108.113.237
10.109.46.225
172.17.12.146
10.123.35.127
10.123.44.74
172.17.12.212
172.17.12.128
172.17.12.33
172.17.12.189



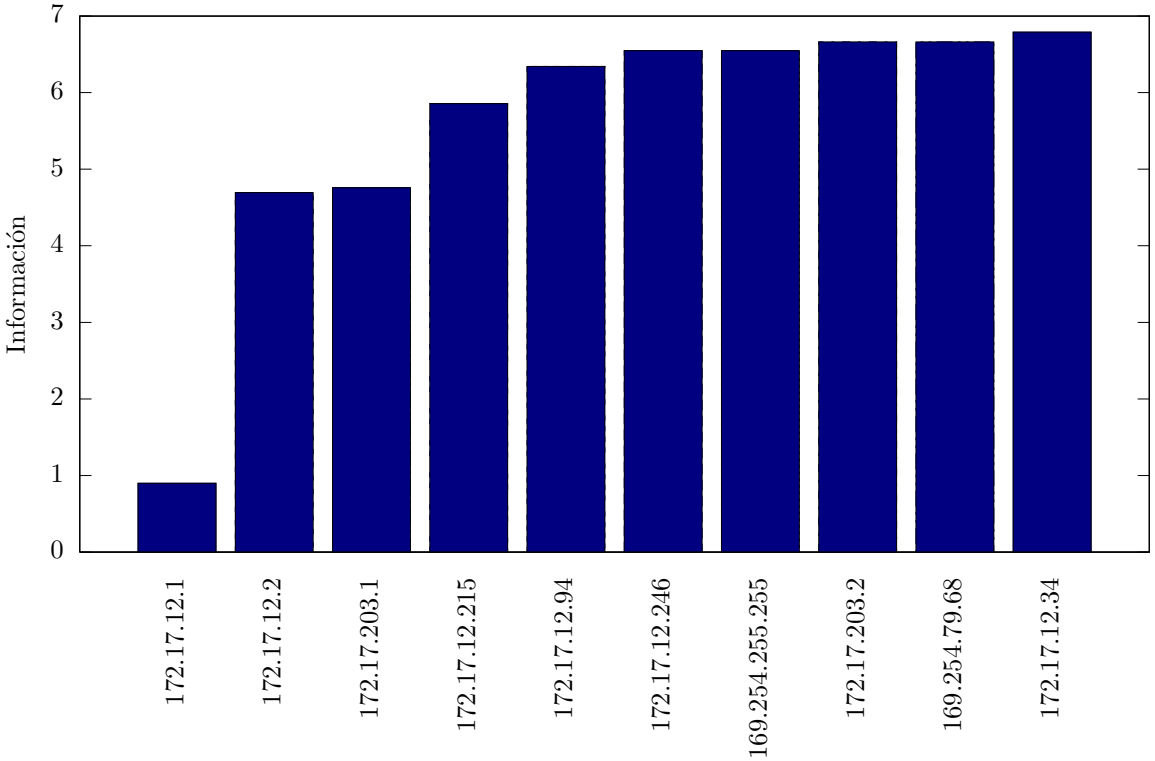
3.2.1. Información de los símbolos de la fuente de información S_{src}

Donde $S_{src} = \{$direcciones IP origen en paquetes ARP *who-has*$\}$.

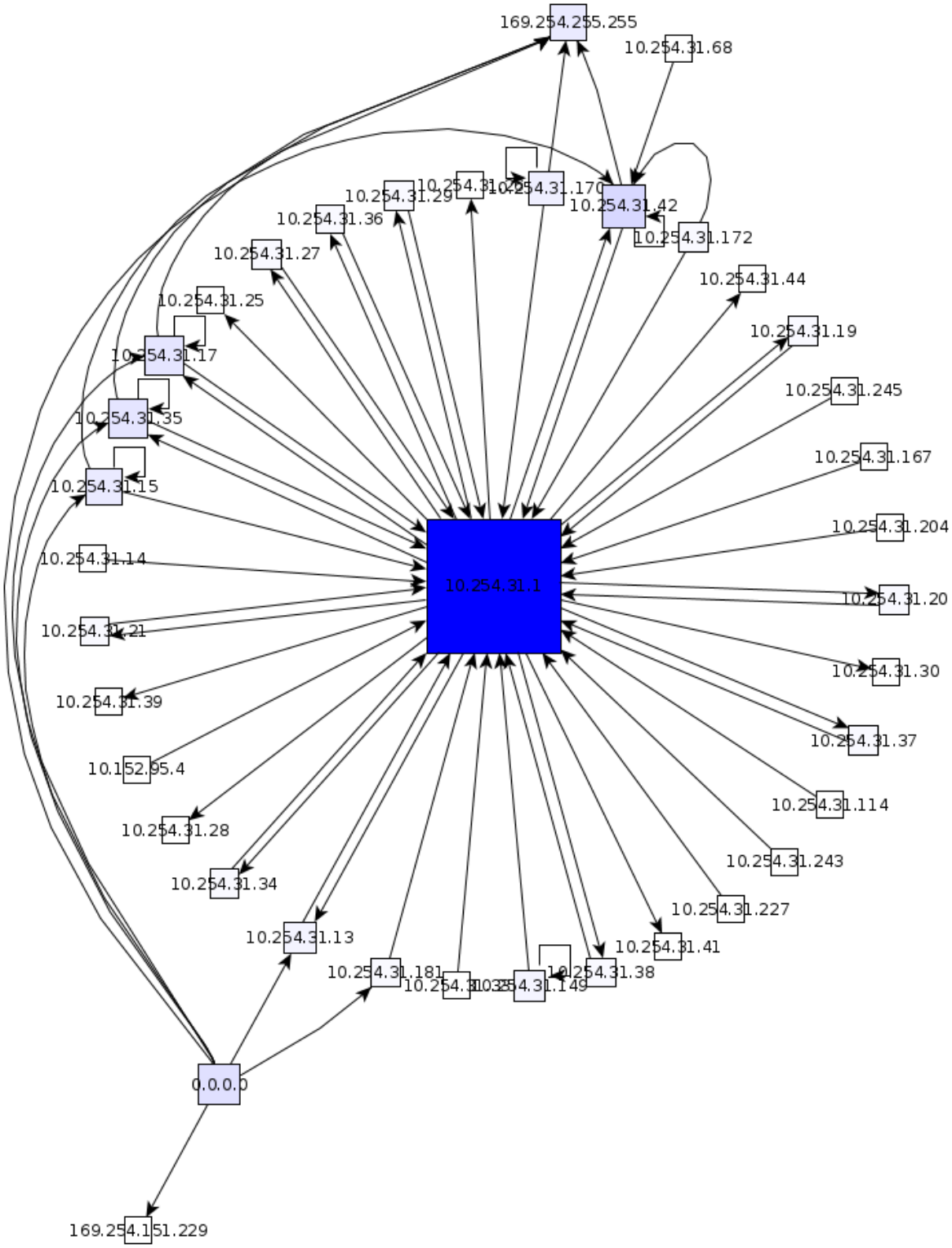


3.2.2. Información de los símbolos de la fuente de información S_{dst}

Donde $S_{dst} = \{$direcciones IP destino en paquetes ARP *who-has*$\}$.

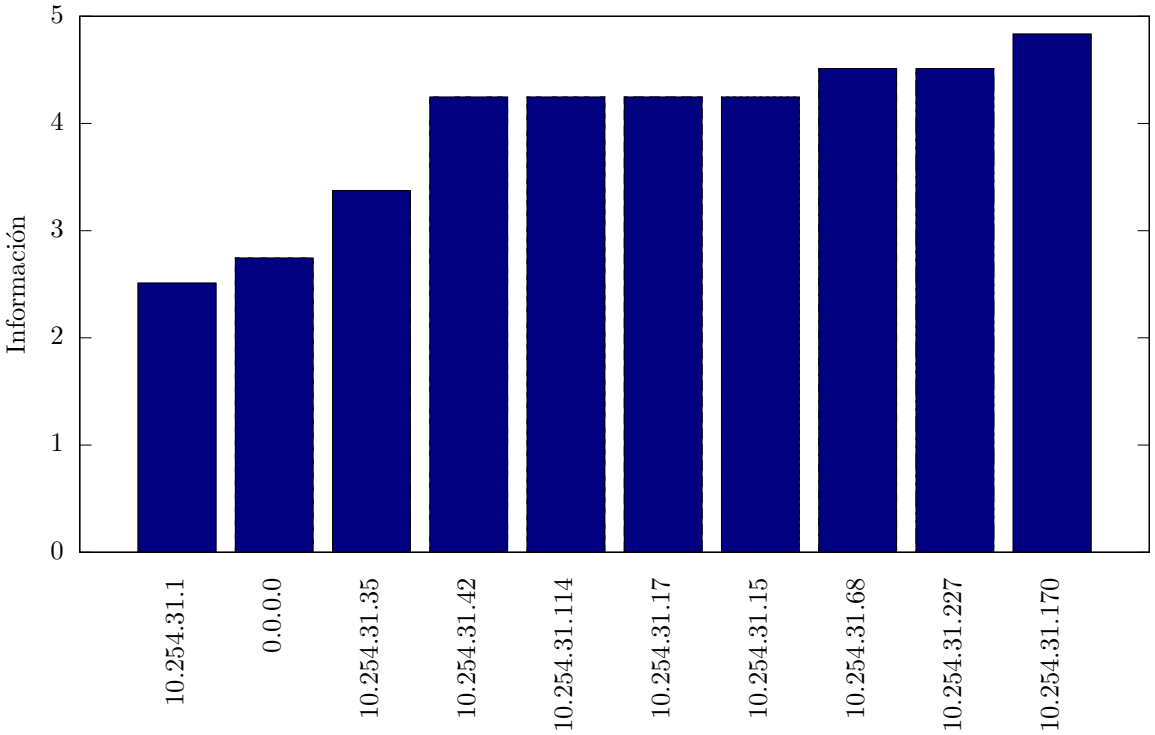


3.3. Red *Starbucks*



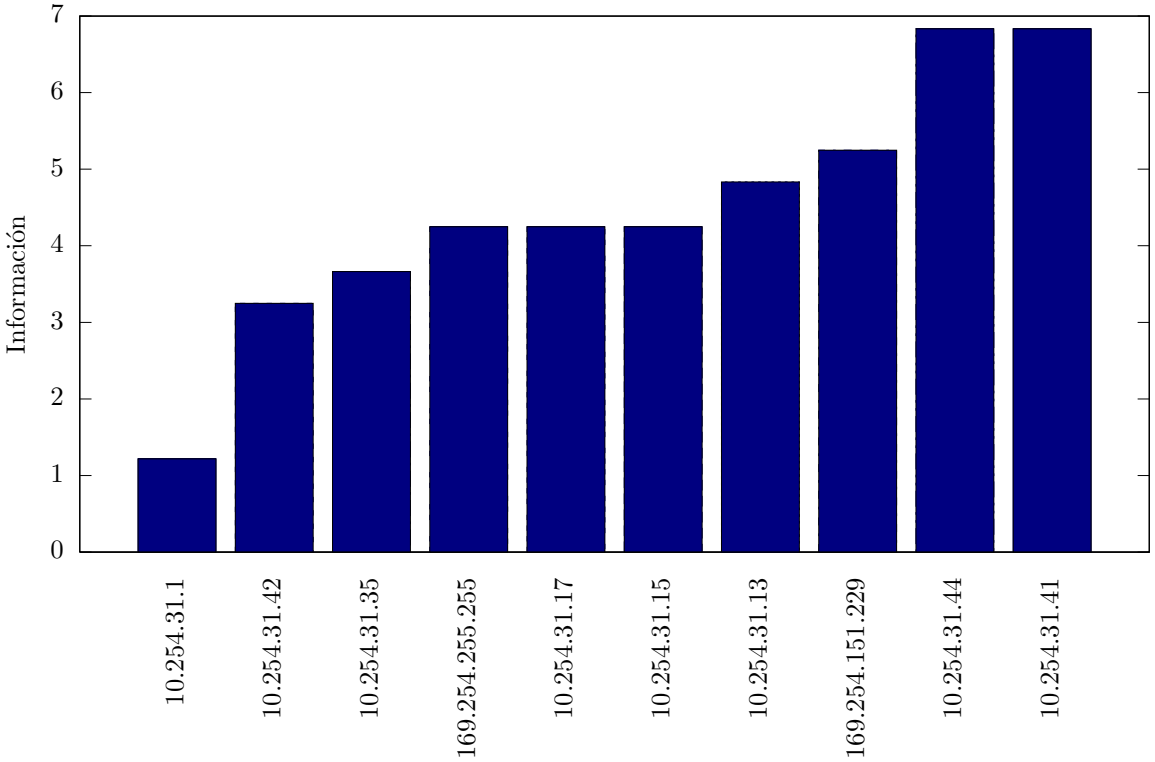
3.3.1. Información de los símbolos de la fuente de información S_{src}

Donde $S_{src} = \{$direcciones IP origen en paquetes ARP *who-has*$\}$.



3.3.2. Información de los símbolos de la fuente de información S_{dst}

Donde $S_{dst} = \{$direcciones IP destino en paquetes ARP *who-has*$\}$.



3.4. Entropías calculadas

Red	Fuente de información modelada S	Entropía $H(S)$
Alto Palermo	S_{src}	0.109542
Alto Palermo	S_{dst}	3.738743
McDonald's	S_{src}	3.976417
McDonald's	S_{dst}	3.769457
Starbucks	S_{src}	4.142124
Starbucks	S_{dst}	3.271891

4. Discusión

4.1. Datos encontrados

4.1.1. Paquete ARP con IP fuente 0.0.0.0

Podemos detectar en la red de MC Donalds paquetes ARP Who-Has con ip fuente 0.0.0.0. La causa de estos ips es debido a lo siguiente: Cuando un cliente se conecta a un red que posee un servidor DHCP y quiere recibir una IP de esta, manda una petición con su ID en forma de broadcast para que lo detecte el servidor. Una vez detectado por el servidor, este manda una o varias ofertas de IP's a ese ID. El cliente eventualmente podría recibir la oferta, tomar uno de esos IP's y extraer la dirección del router. Como el servidor realiza la misma operación con todos los demás clientes que pidan una IP, el cliente debe comprobar que la IP que eligió no la tiene otro cliente. Para esto, coloca en el paquete Who-Has su MAC adress, la ip 0.0.0.0 como fuente para evitar confundir las ARP caches en otros hosts. Si el who-has es respuesto, el cliente rechaza el IP elegido.

5. Conclusión