



DEPARTAMENTO  
DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA



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
Lovisol, Leandro	645/11	leandro@leandro.me
Petaccio, Lautaro José	443/11	lausuper@gmail.com

# Índice

<b>1. Introducción teórica</b>	<b>3</b>
<b>2. Desarrollo</b>	<b>4</b>
<b>3. Resultados</b>	<b>4</b>
3.1. Red <i>Alto Palermo</i> . . . . .	4
3.1.1. Información de los símbolos de la fuente de información $S_{src}$ . . . . .	4
3.1.2. Información de los símbolos de la fuente de información $S_{dst}$ . . . . .	5
3.2. Red <i>McDonald's</i> . . . . .	6
3.2.1. Información de los símbolos de la fuente de información $S_{src}$ . . . . .	8
3.2.2. Información de los símbolos de la fuente de información $S_{dst}$ . . . . .	9
3.3. Red <i>Starbucks</i> . . . . .	10
3.3.1. Información de los símbolos de la fuente de información $S_{src}$ . . . . .	10
3.3.2. Información de los símbolos de la fuente de información $S_{dst}$ . . . . .	11
3.4. Entropías calculadas . . . . .	12
<b>4. Discusión</b>	<b>12</b>
4.1. Fenómenos Destacables . . . . .	12
4.1.1. Paquetes ARP con IP origen 0.0.0.0 . . . . .	12
4.1.2. Paquetes ARP con MAC destino 00:00:00:00:00:00 . . . . .	12
4.1.3. Direcciones en el rango 169.254.0.0/16 . . . . .	12
4.1.4. Misma IP como origen y destino . . . . .	12
<b>5. Conclusión</b>	<b>12</b>

## 1. Introducción teórica

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:

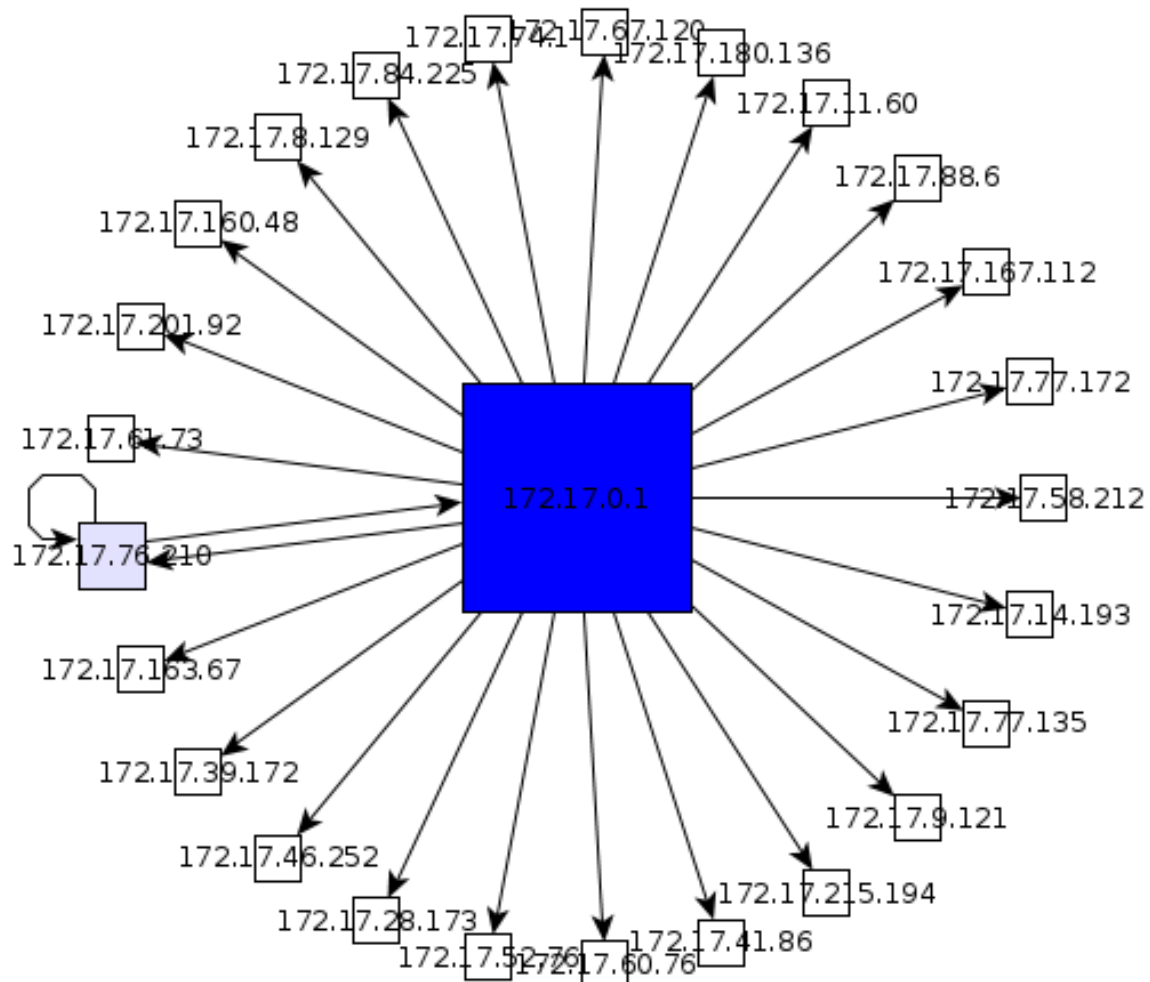
Una máquina en una red quiere mandarle un paquete de datos a otra máquina en la misma red. Para esto, la máquina emisora busca en su tabla local, la dirección MAC asociada a la dirección IP a la cuál quiere mandar el paquete. Si no la encuentra, realiza el broadcasts de la petición ARP, la cual llegará 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

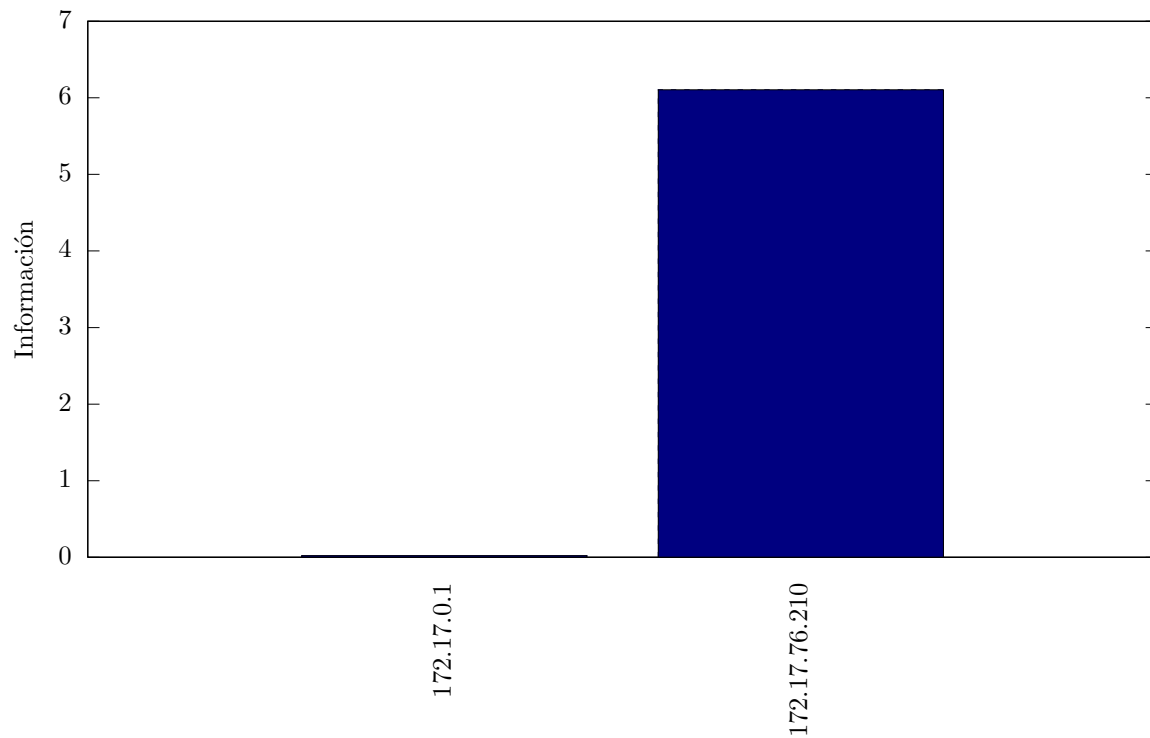
## 3. Resultados

### 3.1. Red *Alto Palermo*



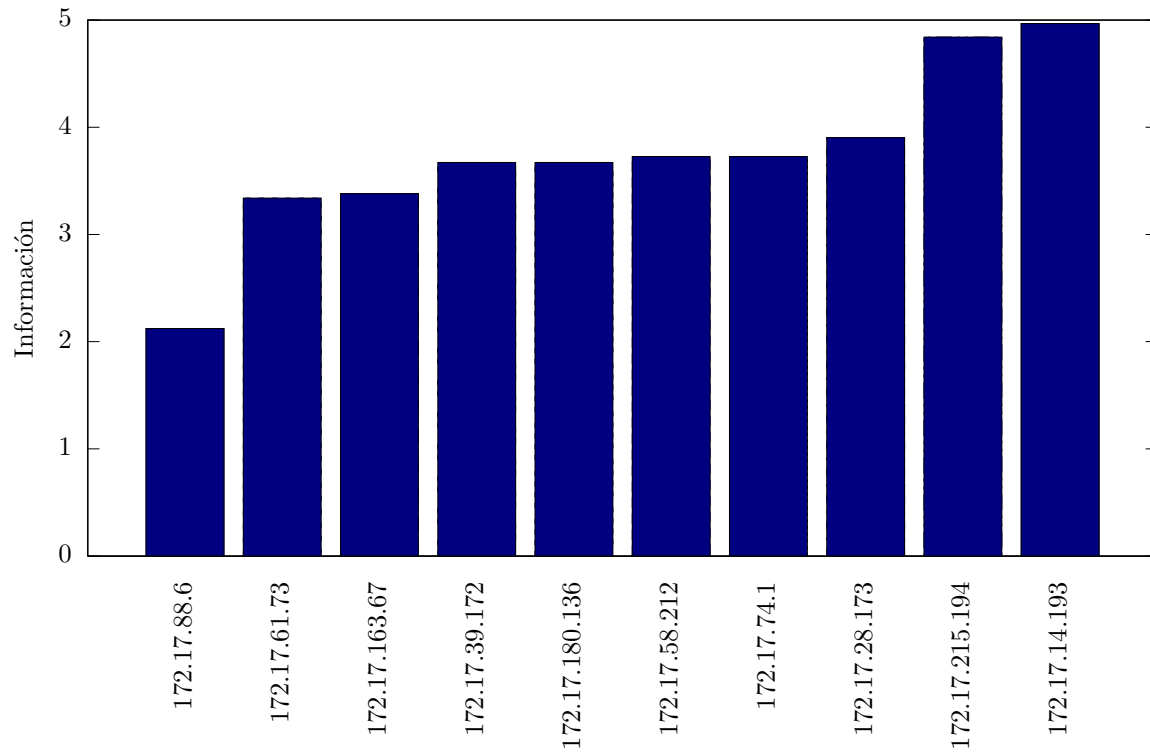
#### 3.1.1. Información de los símbolos de la fuente de información $S_{src}$

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

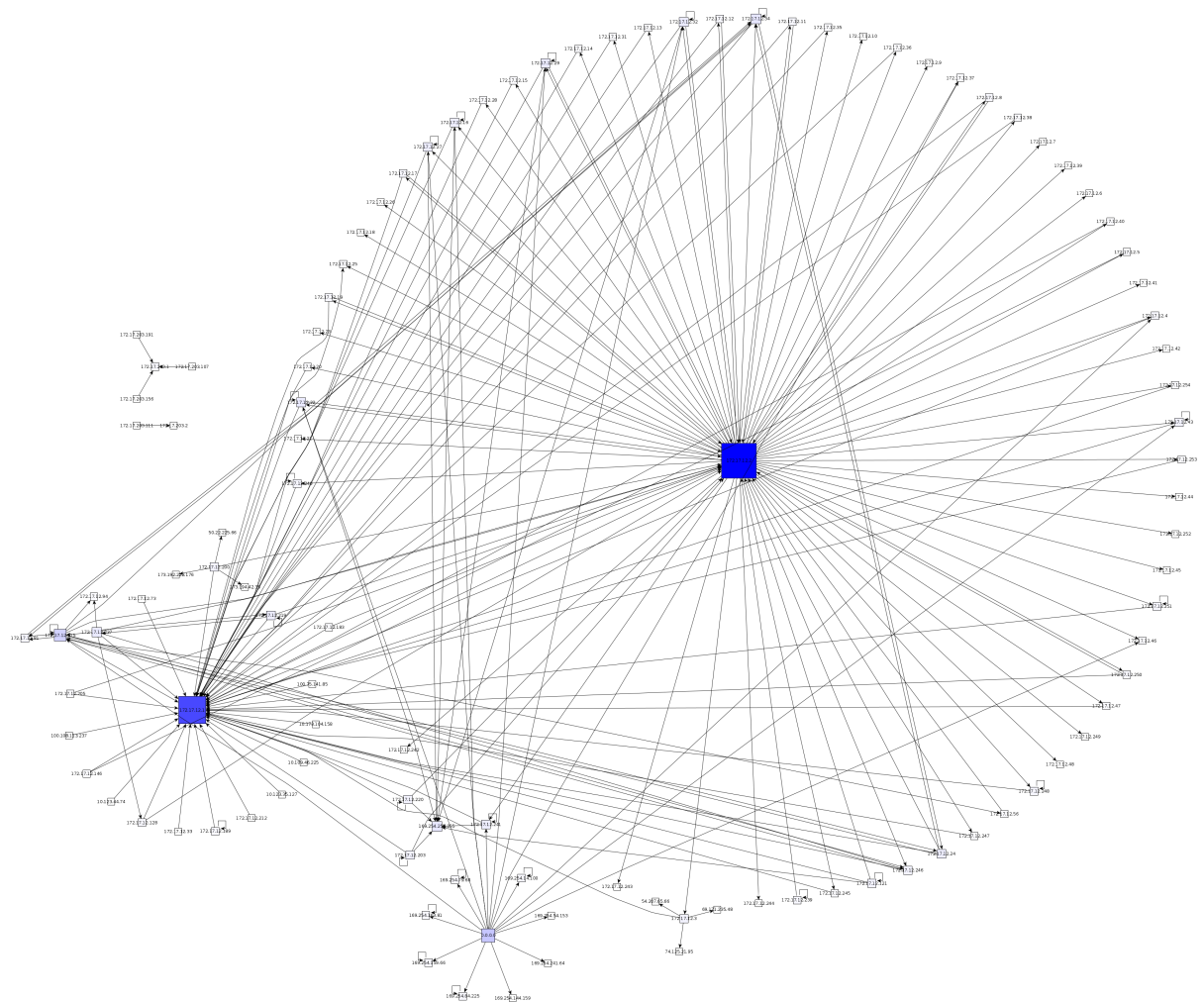


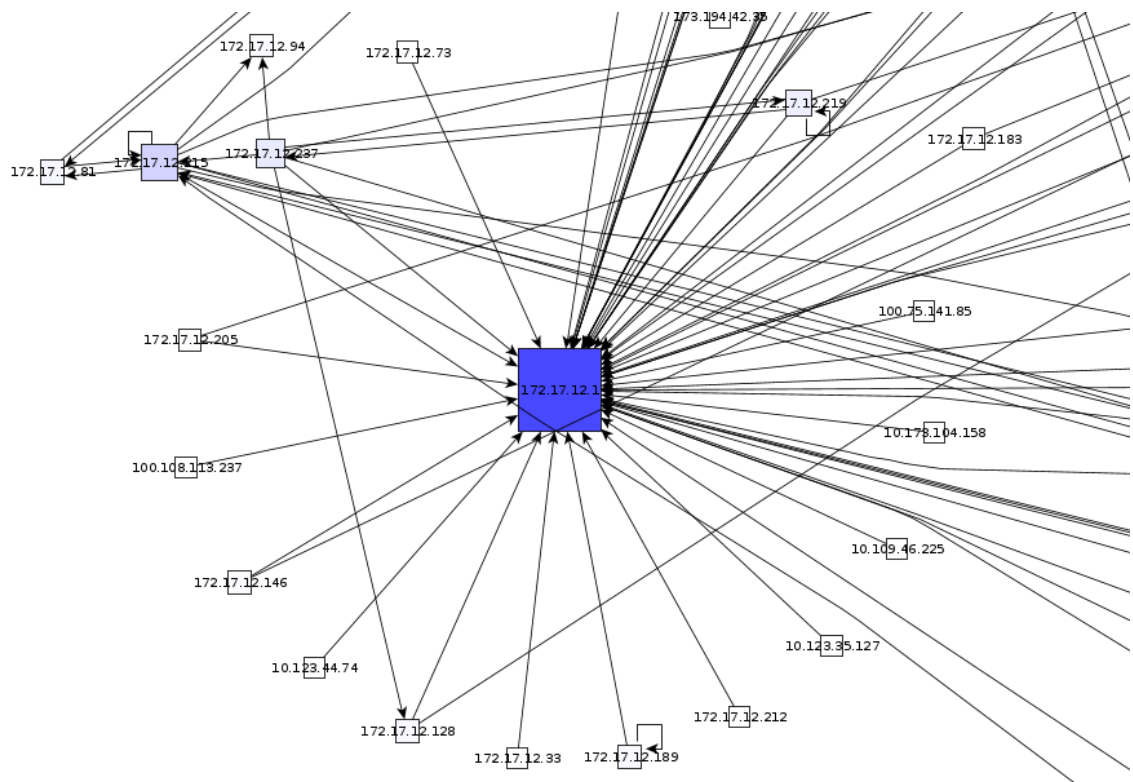
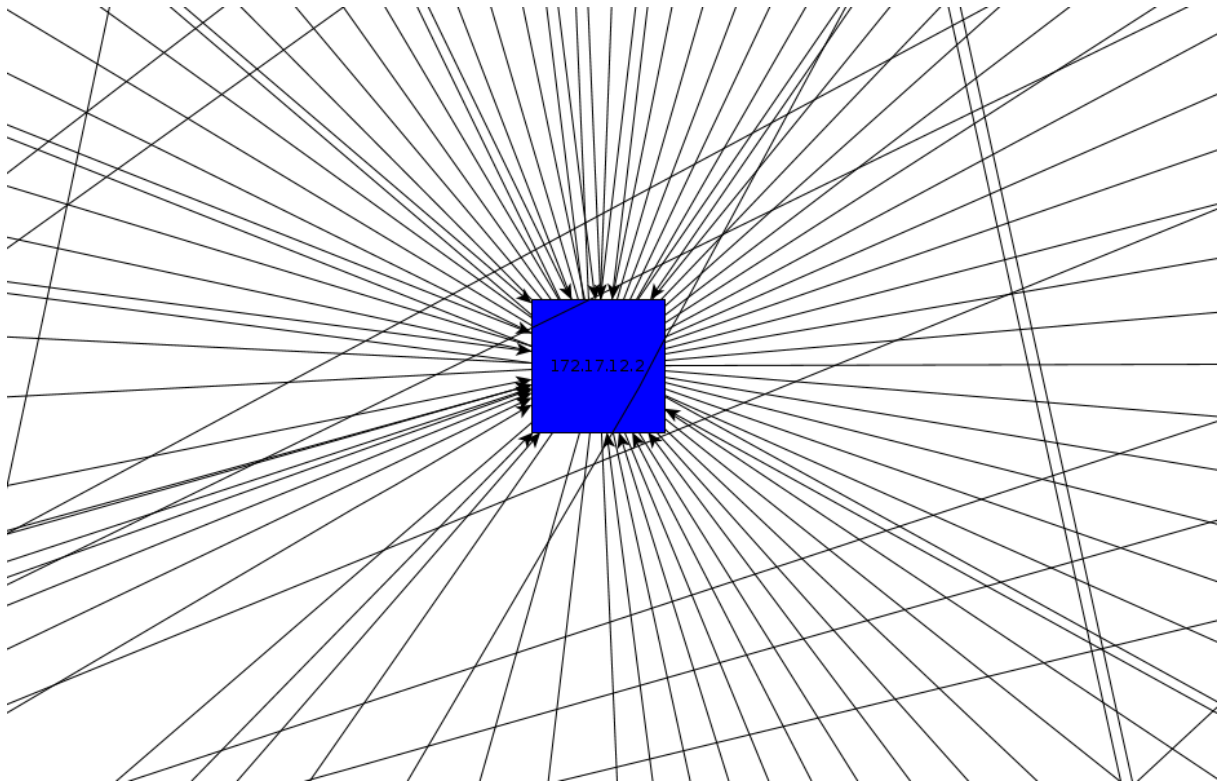
### 3.1.2. Información de los símbolos de la fuente de información $S_{dst}$

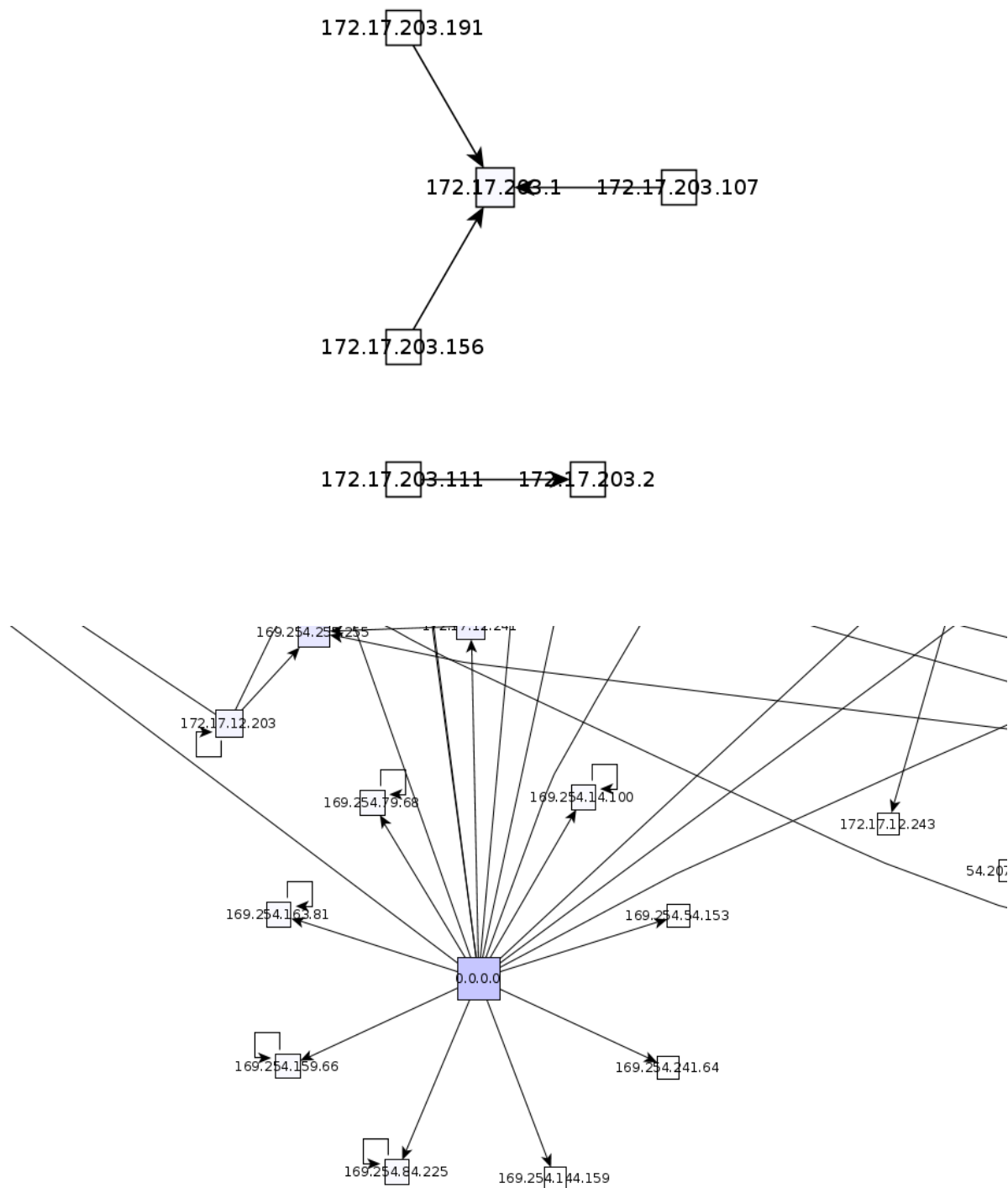
Donde  $S_{dst} = \{\text{direcciones IP destino en paquetes ARP } who\text{-}has\}$ .



### 3.2. Red *McDonald's*



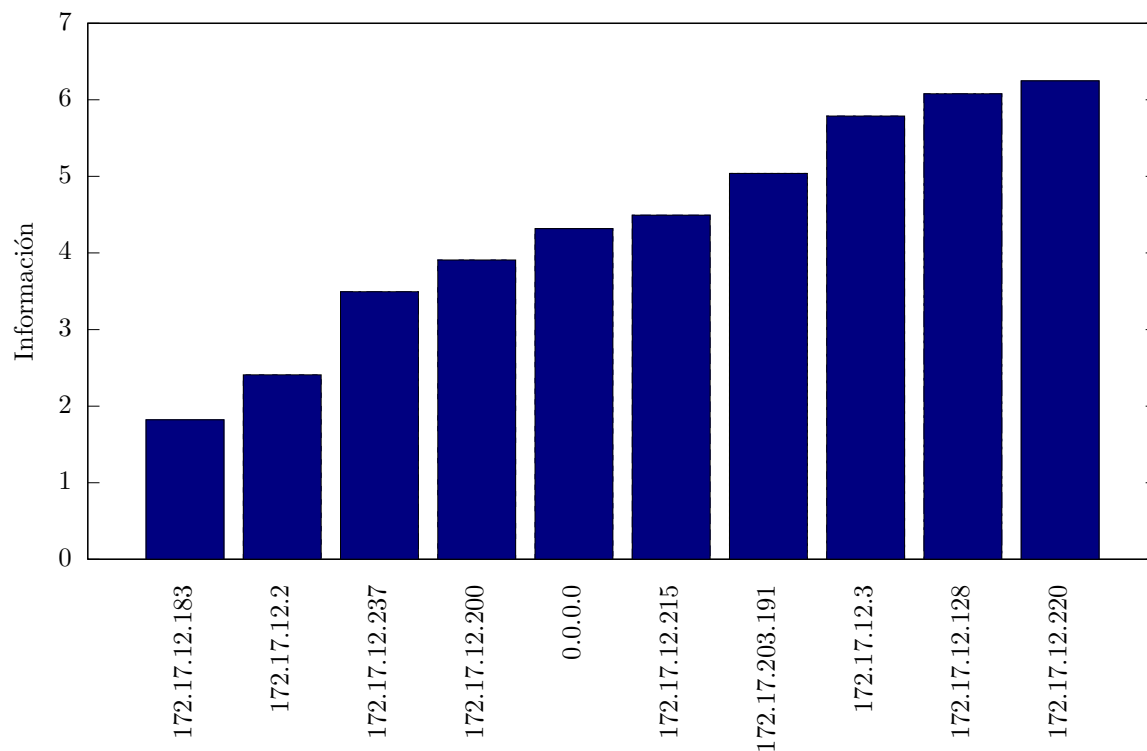




### 3.2.1. Información de los símbolos de la fuente de información $S_{src}$

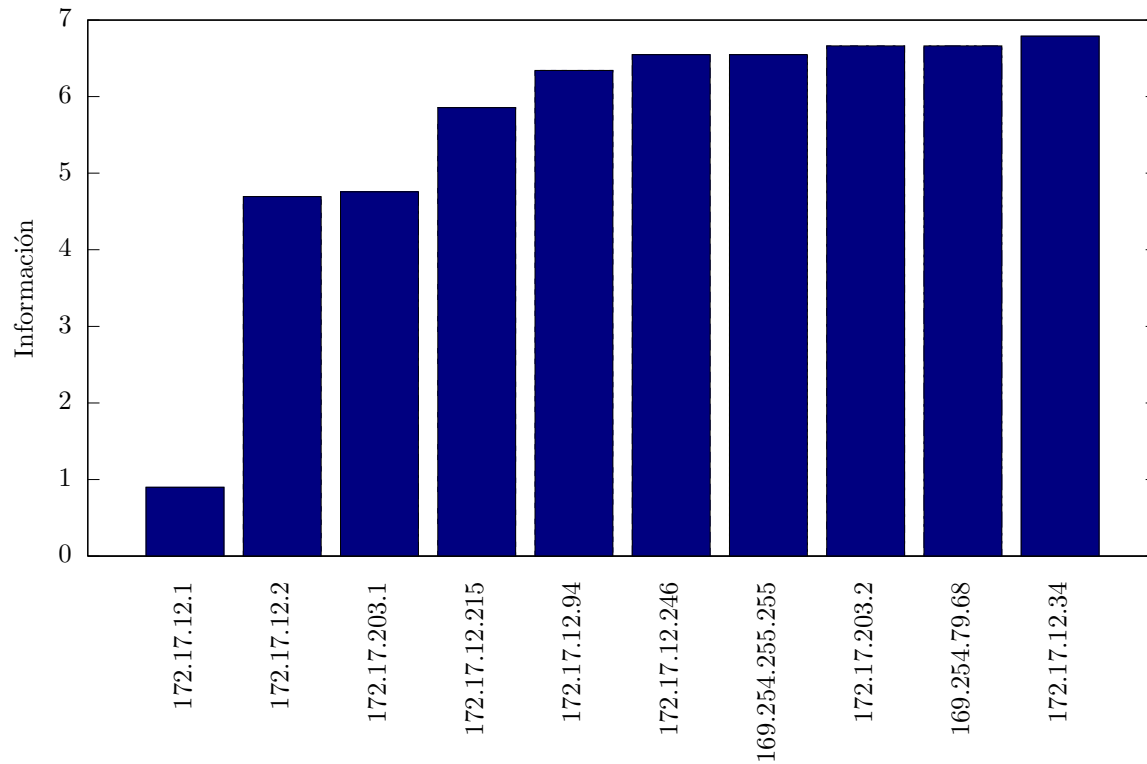
Donde  $S_{src} = \{\text{direcciones IP origen en paquetes ARP } who-has\}$ .



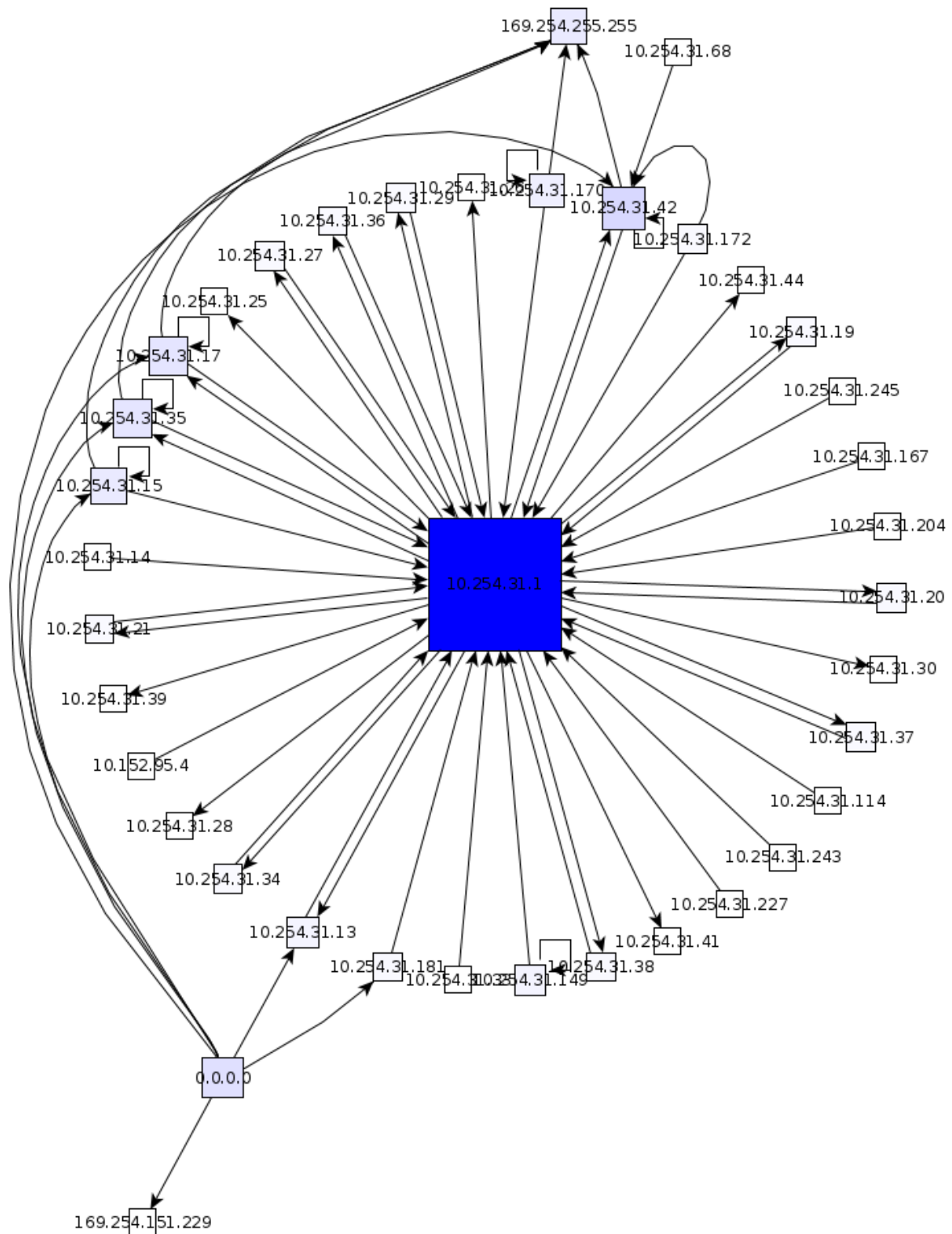


### 3.2.2. Información de los símbolos de la fuente de información $S_{dst}$

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

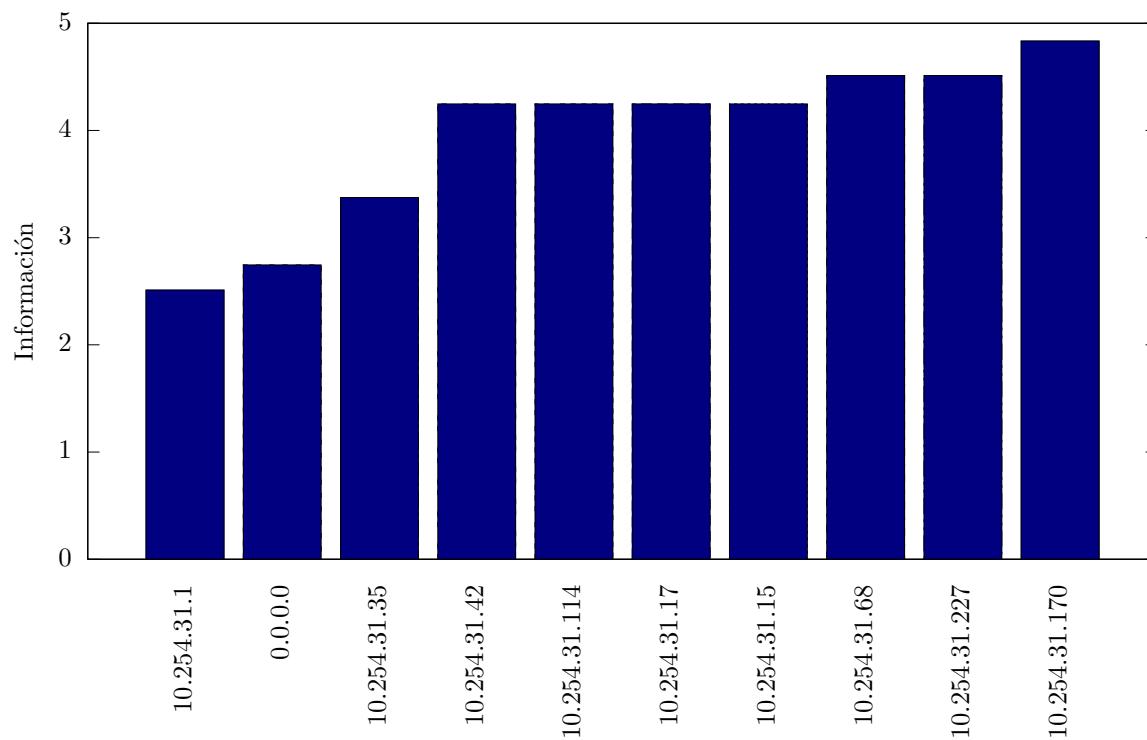


### 3.3. Red Starbucks



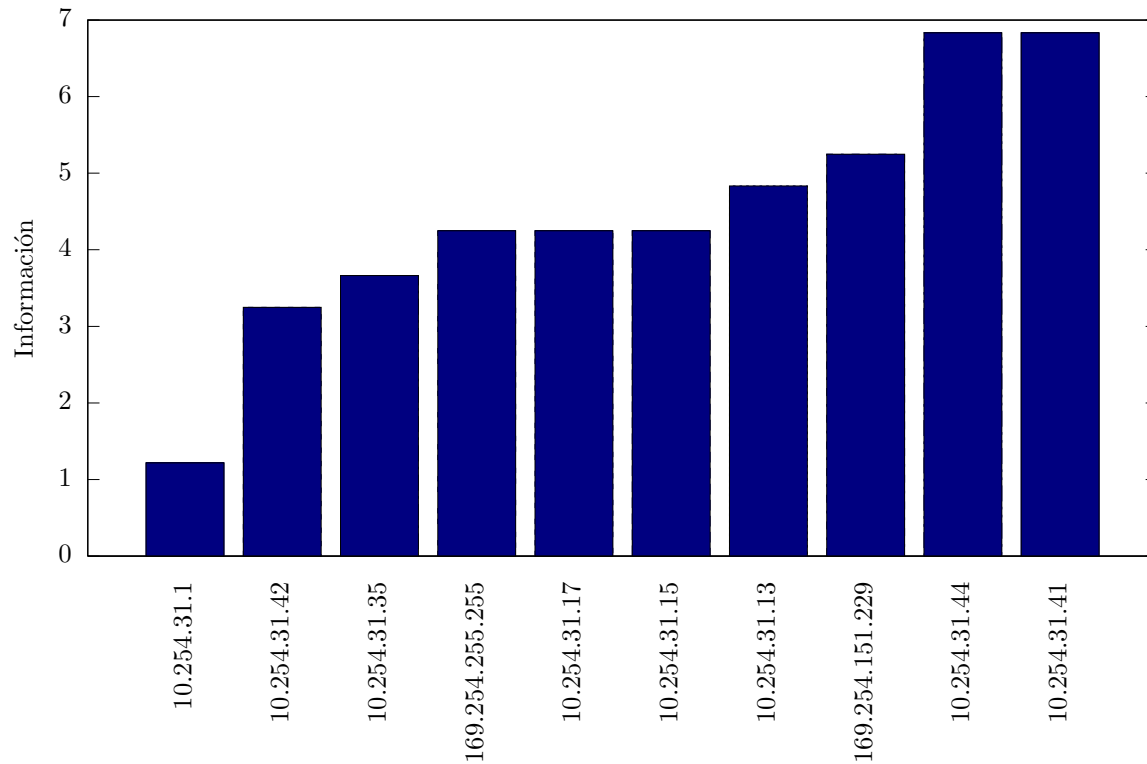
#### 3.3.1. Información de los símbolos de la fuente de información $S_{src}$

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



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

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



### 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. Fenómenos Destacables

#### 4.1.1. Paquetes ARP con IP origen 0.0.0.0

Podemos detectar en la red de Mc Donalds y en la de Starbucks paquetes ARP **who-has** con IP origen 0.0.0.0. El motivo de uso de esta IP es el 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, envía un paquete **who-has** con su MAC adress y 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.

#### 4.1.2. Paquetes ARP con MAC destino 00:00:00:00:00:00

Esta MAC es utilizada como dirección de destino para los paquetes llamados de *ARP gratuito*<sup>1</sup>. Este modo de uso del protocolo es mayormente para detectar conflictos de IP en la red o actualizar información en las tablas de los vecinos. La dirección en cuestión se interpreta como broadcast, pero fácilmente distinguible de los paquetes ARP estándar.

#### 4.1.3. Direcciones en el rango 169.254.0.0/16

#### 4.1.4. Misma IP como origen y destino

## 5. Conclusión

---

<sup>1</sup>[http://wiki.wireshark.org/Gratuitous\\_ARP](http://wiki.wireshark.org/Gratuitous_ARP)