



Trabajo Práctico 1

Wiretapping

19 de abril de 2016

Teoría de las comunicaciones

Integrante	LU	Correo electrónico
Barbeito, Nicolás	147/10	barbeiton@yahoo.com.ar
Interlandi, Daniel	773/00	danielinterlandi@gmail.com
Ladelfa, Hernán Nahuel	318/04	nahueladelfa@gmail.com

Instancia	Docente	Nota
Primera entrega		
Segunda entrega		



Facultad de Ciencias Exactas y Naturales

Universidad de Buenos Aires

Ciudad Universitaria - (Pabellón I/Planta Baja)

Intendente Güiraldes 2610 - C1428EGA

Ciudad Autónoma de Buenos Aires - Rep. Argentina

Tel/Fax: (++54 +11) 4576-3300

<http://www.exactas.uba.ar>

Índice

1. Resumen	2
2. Introducción	2
3. Primera consigna: capturando tráfico	3
3.1. Herramienta	3
3.2. Ejecución	3
4. Resultados	4
4.1. Segunda Consigna: Gráficos y Análisis	4
4.1.1. Red Doméstica	4
4.1.2. Histogramas (de IPs y protocolos)	4
4.1.3. Paquetes capturados e información	5
5. Segunda Consigna: Gráficos y Análisis	8
5.1. Resultados	8
5.1.1. Red Laboral	8
5.1.2. Histogramas (de IPs y protocolos)	8
5.1.3. Paquetes capturados e información	9
6. Conclusiones	10

1. Resumen

El objetivo de este trabajo es utilizar técnicas provistas por la teoría de la información para distinguir diversos aspectos de la red de manera analítica. Además, sugerimos el uso de dos herramientas modernas de manipulación y análisis de paquetes frecuentemente usadas en el dominio de las redes de computadoras: Wireshark y Scapy.

2. Introducción

Se modelaron las redes analizadas como dos fuentes, S y S_1 . La primera tiene como objetivo examinar los protocolos presentes y su importancia en la misma, se toma

$$S = \{s_1 \dots s_n\}$$

donde s_i es $p_i.type$, con p_i el i-ésimo paquete capturado.

El segundo modelo es

$$S_1 = \{s_{1,1} \dots s_{1,n}\}$$

donde $s_{1,i}$ es $p_i.pdst$ (dirección IP destino), con p_i el i-ésimo paquete del protocolo ARP capturado. Este es utilizado para analizar la importancia de los nodos dentro de la red.

Usando estos modelos y los conceptos de información y entropía podemos detectar símbolos destacados en las fuentes (nodos o protocolos según la fuente). La información que otorga un símbolo s_i en una fuente se define como

$$I(s_i) = \log(1/P(s_i))$$

y nos ayuda a detectar que tan frecuente es la emisión de ese símbolo por la fuente. La entropía de una fuente $S = \{s_1 \dots s_n\}$ se define como

$$\sum_S P(s_i)I(s_i) \forall s_i \in S$$

este número da la información media emitida por la fuente. Indica que tan desordenada es la aparición de los símbolos.

Un concepto fundamental es el del protocolo ARP. Este sirve para relacionar direcciones de nivel de red (IP) con direcciones de nivel de enlace (MAC). Cuando un equipo desea mandar un paquete a una dirección IP dada, necesita ubicar el mismo a nivel de enlace, entonces envía un ARP-request mediante broadcast requiriendo una respuesta del poseedor de la dirección IP, luego, si existe, el nodo que tenga esa IP responderá usando un paquete ARP reply a quién realizó la consulta con su dirección MAC. De esta manera, interceptando paquetes ARP se puede detectar qué nodos activos hay en una red.

3. Primera consigna: capturando tráfico

3.1. Herramienta

Para realizar las capturas de las redes, se desarrollo un script en el lenguaje Python integrado con la herramienta Scapy. Este script escucha pasivamente la red capturando los paquetes que son almacenados en distintos archivos para su posterior análisis.

En los archivos se guarda la información, probabilidad y entropía de las 2 fuentes elegidas. Por tipo de protocolo para los paquetes Ethernet y por IP para la captura de paquetes ARP.

Un 3 archivo de formato json, contiene la información de manera organizada para poder ser leído por otro script desarrollado utilizado para generar distintos gráficos.

Este segundo script genera gráficos como histogramas, de torta y grafos según paquetes ARP enviados.

3.2. Ejecución

Para la ejecución de la herramienta, debemos ejecutar los siguiente comandos desde una terminal en el sistema operativo Linux.

```
$ sudo ./sniffer.py <outputfile> <timeout>
```

Para la ejecución del graficador:

```
$ sudo ./plot.py <outputfile>
```

4. Resultados

4.1. Segunda Consigna: Gráficos y Análisis

4.1.1. Red Doméstica

Para la primera captura, se eligió una red doméstica de uno de los integrantes del grupo. La captura duro 30 minutos aproximados. Al ser una red pequeña podemos distinguir fácilmente los nodos destacados. La Figura 1 muestra 2 nodos destacados 192.168.0.1 que corresponde al router y el nodo 192.168.0.27 correspondiente al PC desde donde se tomaron las capturas.

Topografía de la red segun paquetes ARP enviados

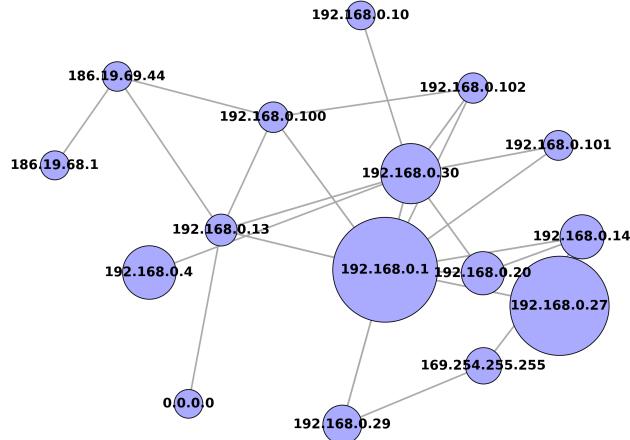


Figura 1: Mi Figura

4.1.2. Histogramas (de IPs y protocolos)

Histograma de entropía de direcciones IP en la red

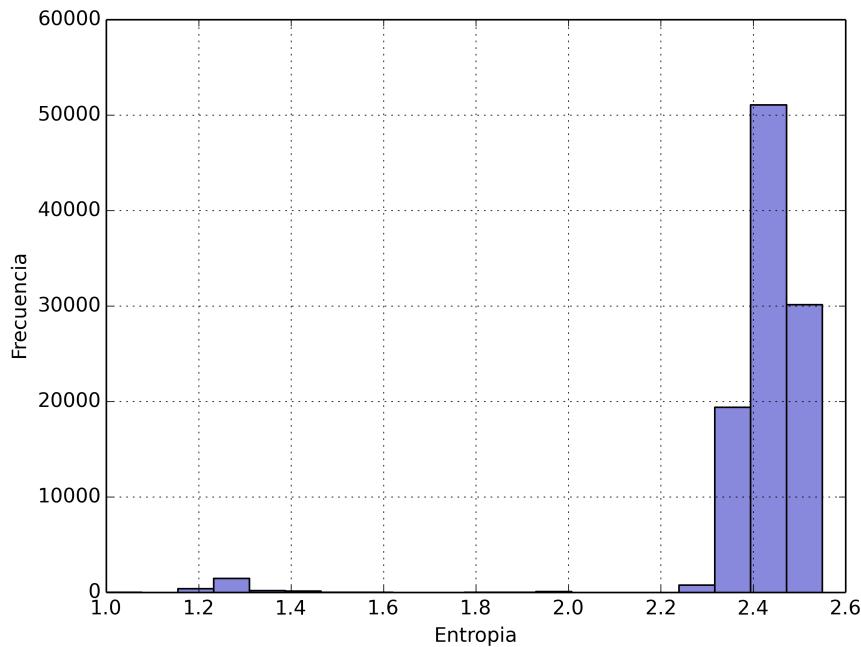


Figura 2: Mi Figura

Histograma de entropía de tipos de paquete en la red

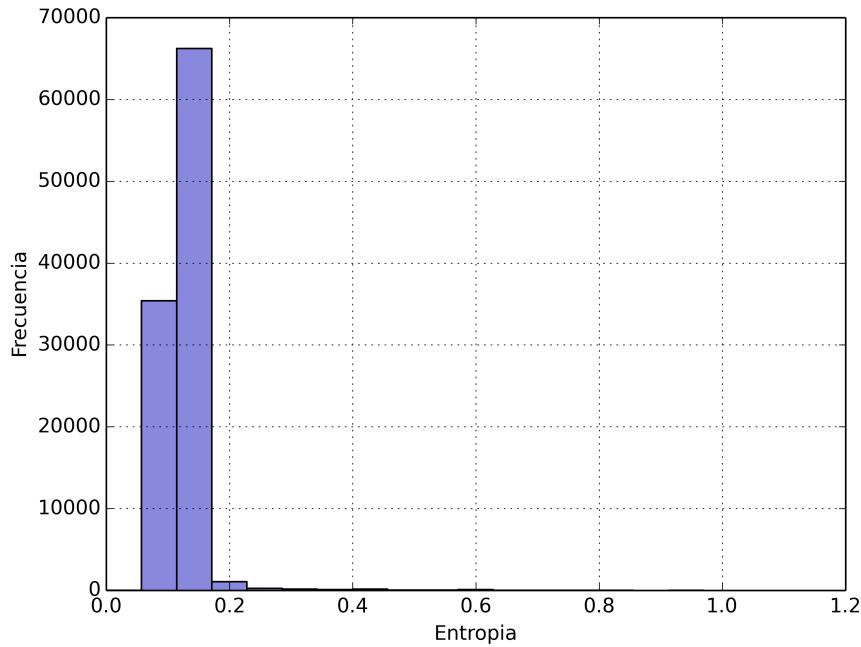


Figura 3: Mi Figura

4.1.3. Paquetes capturados e información

Los gráficos de torta, nos permiten ver la relación entre la cantidad de paquetes y la información que proveen cada nodo en la red. En los primeros 2 gráficos 4. 5. se toma como fuente las ips de la red. Podemos notar que los nodos mencionados anteriormente son los mas frecuentes y por lo tanto los que menos información tienen.

En los siguientes 2 gráficos 6. 7. la fuente es la indicada en la cátedra. Vemos que el protocolo que mas se repite es el IP con un porcentaje muy superior al resto y aportando información casi nula.

Cantidad de paquetes en la red por IP

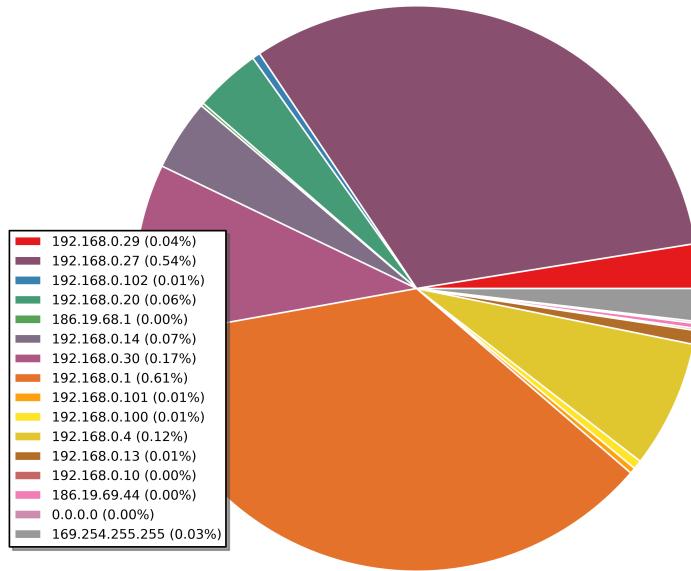


Figura 4: Mi Figura

Informacion por IP en la red

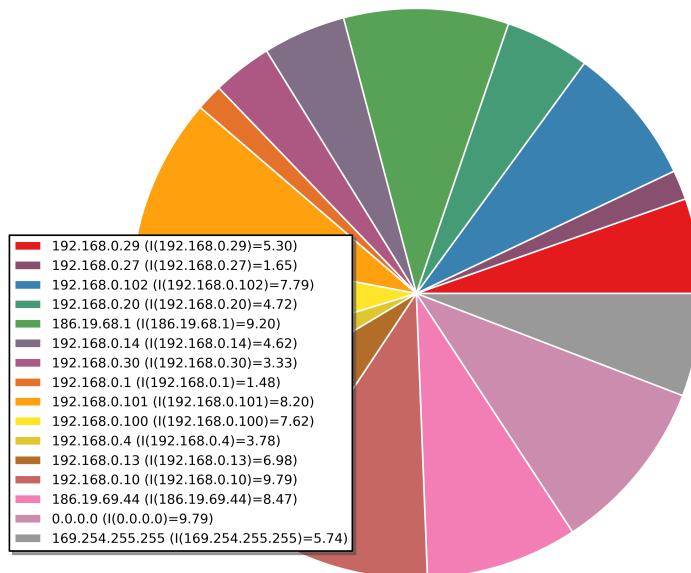


Figura 5: Mi Figura

Cantidad de paquetes en la red por tipo

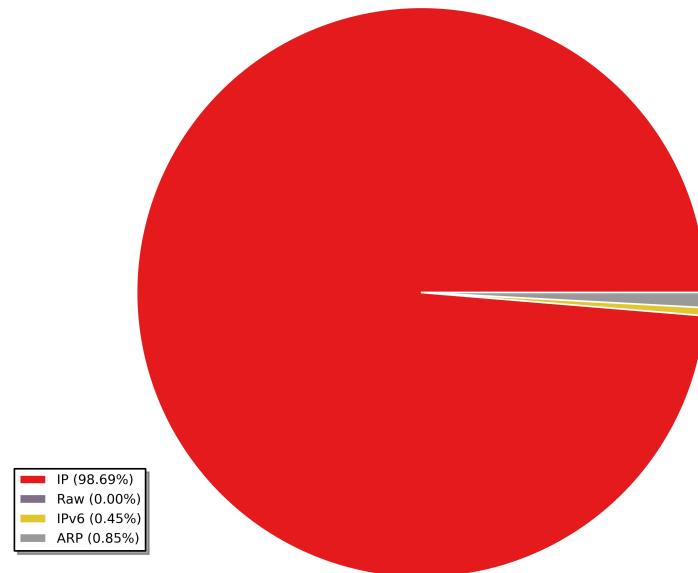


Figura 6: Mi Figura

Informacion por tipo de paquete en la red

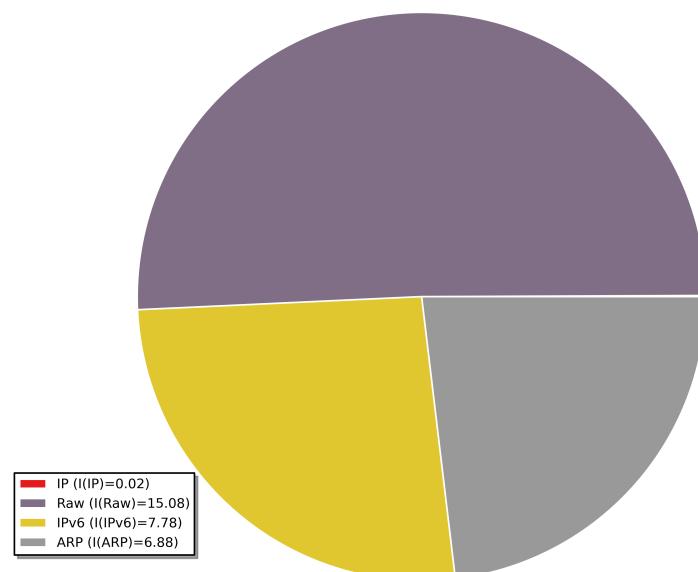


Figura 7: Mi Figura

5. Segunda Consigna: Gráficos y Análisis

5.1. Resultados

5.1.1. Red Laboral

Con las capturas de esta red, se puede notar la gran cantidad de nodos y tráfico de paquetes. El gráfico de topología era tan extenso que decidimos no ponerlo.

5.1.2. Histogramas (de IPs y protocolos)

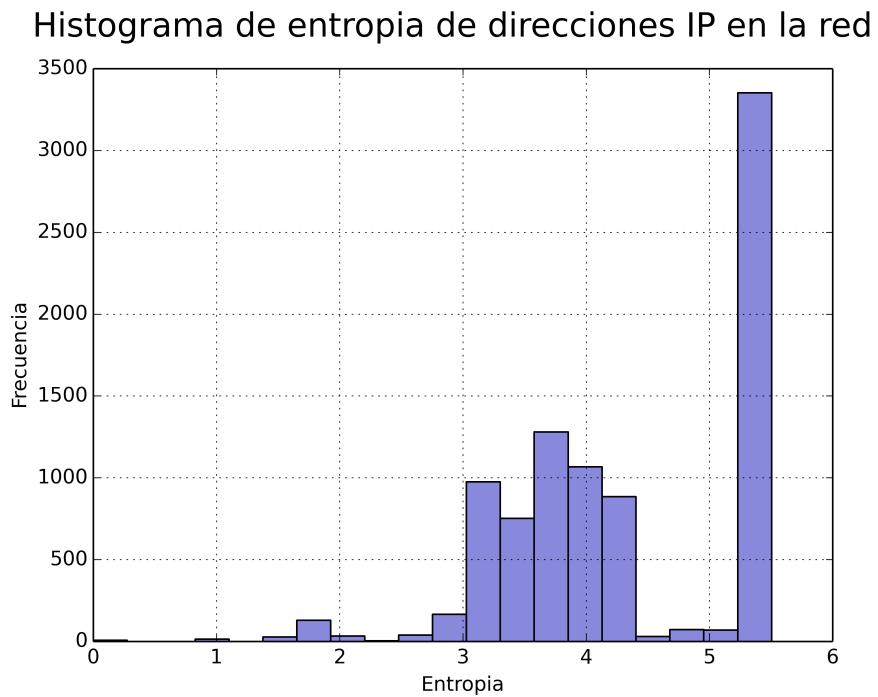
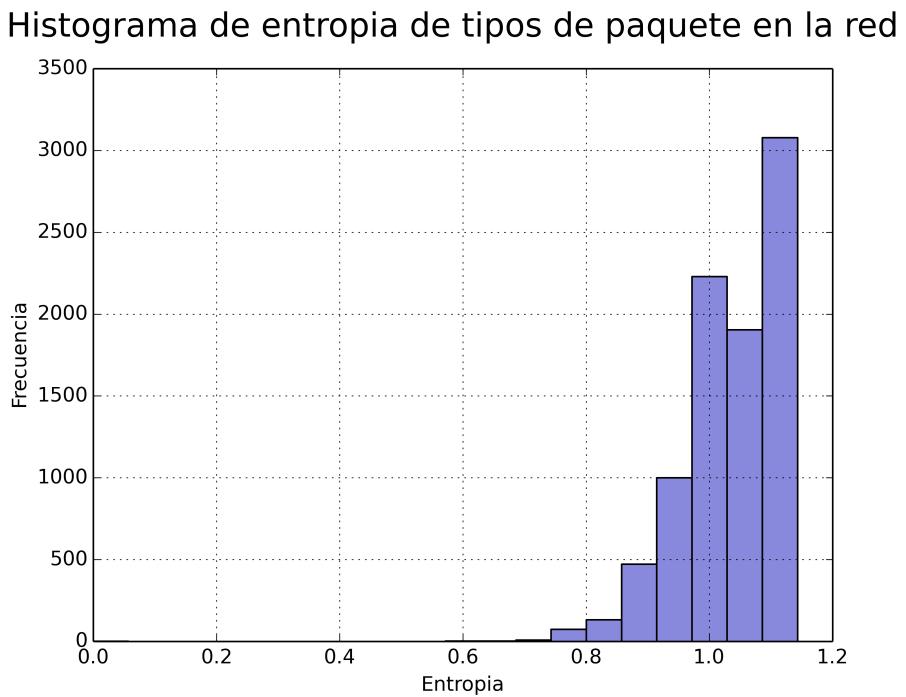


Figura 8: Mi Figura



5.1.3. Paquetes capturados e información

Si bien es una red grande, se puede ver en los gráficos que hay 2 nodos que distinguen del resto 192.168.26.43 con el 0.2% y el 192.168.26.1 con el 0.17%. Se presume que esos nodos tienen que ser routers [10](#) [11](#).

En los gráficos de protocolos se vuelve a repetir que el protocolo IP es el mas frecuente. Pero tambien se observa gran cantidad de paquetes IPv6 [12](#) [13](#).

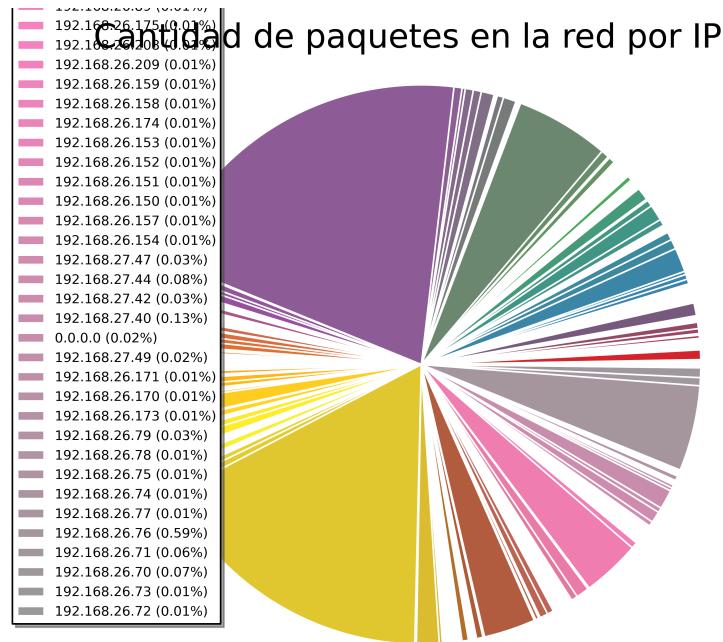


Figura 10: Mi Figura

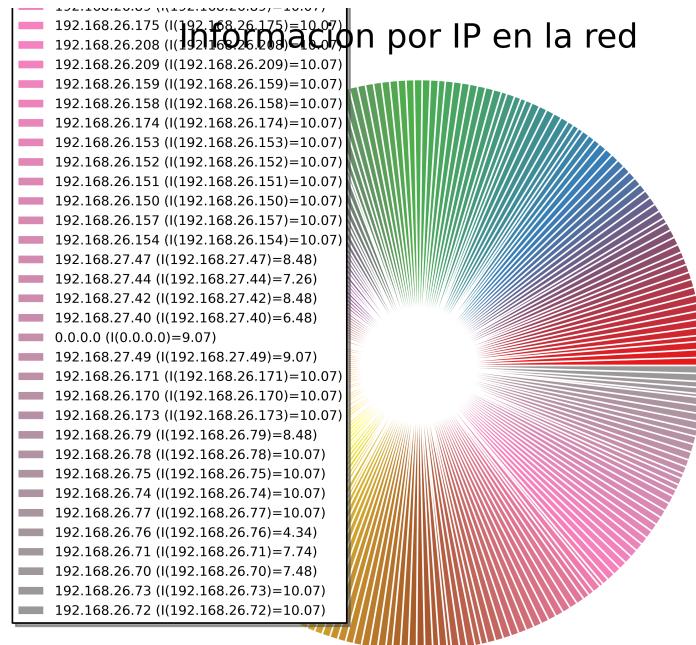


Figura 11: Mi Figura

Cantidad de paquetes en la red por tipo

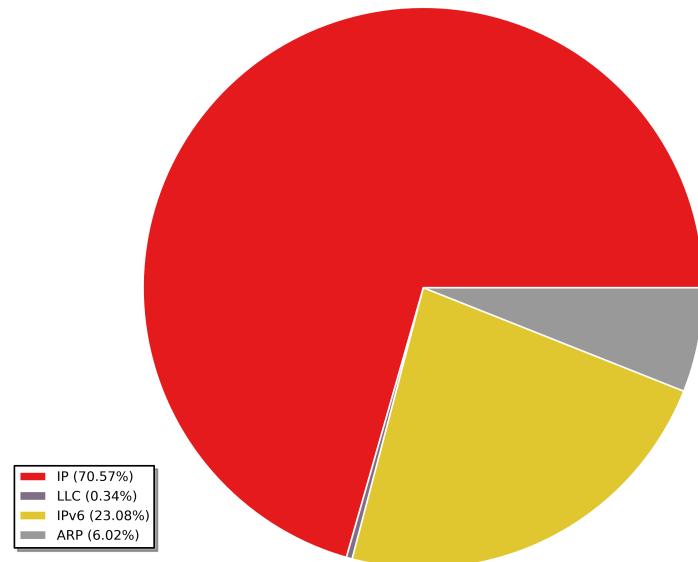


Figura 12: Mi Figura

Informacion por tipo de paquete en la red

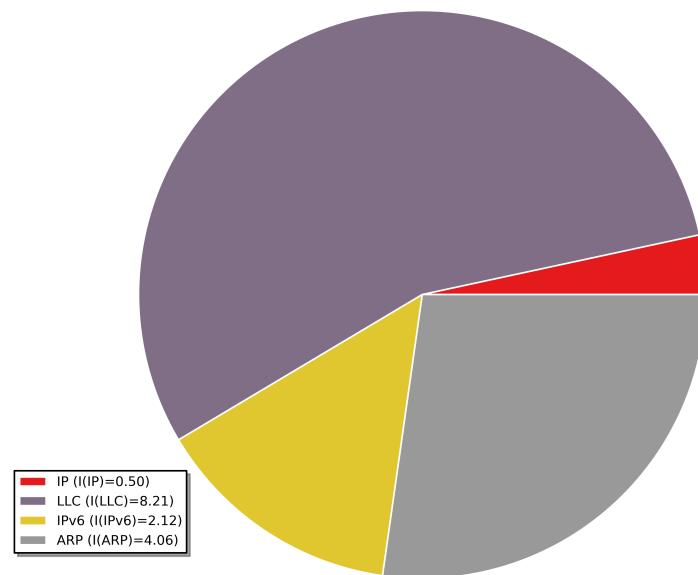


Figura 13: Mi Figura

6. Conclusiones