Teoría de las Comunicaciones

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

Trabajo Práctico 1

Wiretapping

Integrante	LU	Correo electrónico
Dabbah, Julián	15/09	djulius@gmail.com
Fernández Abrevaya, Victoria	710/10	vabrevaya@gmail.com
González, Sergio	723/10	sergiogonza90@gmail.com

Reservado para la cátedra

Instancia	Docente	Nota
Primera entrega		
Segunda entrega		

Índice

Resumen

En el presente trabajo estudiaremos el comportamiento de una red a nivel de enlace, enfocándonos en la relación entre esta capa y la capa superior. Para esto analizaremos los paquetes del protocolo ARP enviados a través de una red local, escuchando pasivamente durante varias horas la red seleccionada. Esta información va a ser utilizada luego para ver, a través de grafos e histogramas, cuáles son los nodos significativos dentro de la misma. A su vez, utilizaremos los conceptos de entropía e información para caracterizar las redes estudiadas, tomando los símbolos de la fuente de alguna manera conveniente. Tanto para el envío de paquetes ARP, como para la captura de datos de la red, utilizaremos las herramientas *Wireshark* y *Scapy*.

Los experimentos serán realizados en cuatro tipos de redes distintos. Los resultados obtenidos son los esperados según el uso que se le da a cada una de estas redes.

Palabras clave: ARP, Teoría de la Información, Entropía, Scapy, Wireshark, Nivel de Enlace, IP, MAC, LAN.

1. Introducción

El presente trabajo práctico tiene como objetivo estudiar el comportamiento de una red a nivel de enlace (analizando principalmente el vínculo de este nivel con la capa superior). Para ello vamos a observar el funcionamiento del protocolo ARP dentro de una determinada red: buscamos caracterizar la misma observando solamente los mensajes enviados a través este protocolo. A su vez, relacionaremos la red estudiada con los conceptos aprendidos dentro del campo de la teoría de la información: utilizando la entropía de una red local (tomando como fuente de información el modelo explicado más adelante) vamos a caracterizar el funcionamiento de la misma, centrándonos en cuales son los nodos distinguidos en ella.

ARP (*Address Translation Protocol*) es el protocolo encargado de mapear direcciones de nivel 3 a direcciones de nivel 2 (nivel físico). Comunmente se utiliza para traducir direcciones IP a direcciones MAC, aunque el protocolo permite asociar otros tipos de direcciones. En este trabajo nos concentraremos solamente en el caso mencionado.

Para construir asociaciones IP-MAC se envía un paquete ARP consistente, entre otros, de los siguientes campos:

- Tipo de mensaje (*"who-is"* / *"is-at"*)
- IP del host que envía el mensaje
- MAC del host que envía el mensaje
- IP del host destino
- MAC del host destino

Si la máquina A quiere comunicarse con B, conociendo solamente su dirección IP, deberá enviar un mensaje ARP de manera *broadcast*, del tipo *who-is*, con la IP de B dentro del campo IP-destino. El host cuya IP se corresponda con el mensaje contestará entonces con un ARP del tipo *is-at*, indicando su dirección a nivel de enlace. Este último mensaje se envía solamente a la IP que desea conocer la MAC, por lo cual sólo puede ser escuchado por la máquina que preguntó. A través del envío de estos paquetes, cada host puede armar dinámicamente una caché de asociaciones IP-MAC. El hecho de que los mensajes *who-has* sean enviados de manera *broadcast* nos permitirá escucharlos fácilmente, para poder sacar conclusiones a partir del uso que se haga de ellos. En general las tablas ARP tienen vigencia por aproximadamente 15 minutos, por lo que se esperan ver mensajes ARP relativamente seguido.

El primer paso para cumplir con los objetivos mencionados será implementar una función que, dada una dirección IP, pregunte con qué dirección MAC se corresponde, y la muestre en pantalla si es que obtuvo respuesta. Para esto utilizaremos la herramienta *scapy*, un programa de manipulación de paquetes. Con esta función analizaremos qué ocurre al suministrarle distintos tipos de direcciones IP.

A continuación implementaremos una función que capture los mensajes ARP, escuchando pasivamente la red local durante un determinado tiempo. Con la información obtenida analizaremos la entropía de la red, utilizando el modelo de fuente explicado en la sección 2.2. A partir de estos datos graficaremos lo observado: grafos dirigidos en los que se indica qué IP mandó mensaje a cual, histogramas con la información calculada según cada IP, entre otros. Esperamos que estos gráficos nos den una caracterización de cada una de las redes estudiadas.

2. Métodos

2.1. Primera Consigna: Implementación de un cliente ARP

El primer paso consiste en implementar una función que, dada una dirección IP, envíe un mensaje ARP a través de la red local preguntando con qué dirección MAC se corresponde. Si recibe respuesta, se muestra por pantalla dicha dirección; en caso contrario se indica que la IP es inexistente, o no puede ser alcanzada desde la red local.

Como mencionamos, esta consigna se implementa utilizando la herramienta *scapy*. Ya que la misma funciona sobre python, programamos la función en este lenguaje. Para el envío del paquete ARP instanciamos un objeto del tipo ARP, y modificamos solamente el campo *pdst*, ya que los otros tienen por defecto los valores que necesitamos (la IP de la máquina que envía, tipo de mensaje *who-has*, etc). El envío en sí se realiza a través de la función *sr* (send and receive), utilizando un timeout de 3 segundos. Esta función devuelve una lista cuyo primer elemento son los paquetes que respondieron, y el segundo los paquetes sin respuestas. Si el primer elemento no es vacío, se devuelven las direcciones MAC recibidas[1]; en caso contrario se indica que dicha dirección no puede ser alcanzada en la red local.

Utilizando la función programada, vamos a analizar qué ocurre al suministrarle distintos tipos de direcciones IP. Todos los casos que mencionamos a continuación fueron probados sobre una red wireless, con IP 192.168.0.3. Los casos testeados fueron los siguientes:

1. Direcciones que pertenecen a la red (para conocer las direcciones IP que se encuentran en la red utilizamos la función *arping*, incluída dentro de *scapy*): 192.168.0.1, 192.168.0.4, 192.168.0.6
2. Direcciones con la máscara de red correcta, pero que no pertenecen a hosts conectados a la misma. Por ejemplo: 192.168.0.2, 192.168.0.5, etc.
3. Misma dirección que la máquina de origen (en este caso, 192.168.0.3).
4. Dirección IP correspondiente a la máquina de origen, según se ve de afuera (utilizando por ejemplo http://www.whatismyip.com/). En este caso dicha dirección fue 24.232.212.124.
5. Dirección broadcast de la red (192.168.0.255)
6. Dirección 0.0.0.0
7. Dirección 255.255.255.255
8. Direcciones inválidas (por ejemplo: 123456789)
9. Direcciones que no pertenecen a la red local (por ejemplo, 173.194.42.35)

Al mismo tiempo utilizaremos la herramienta *wireshark*, para poder ver con más precisión los mensajes que se envían al hacer uso de la función mencionada (como sólo nos interesan los paquetes ARP, utilizaremos un filtro que muestre solamente los mismos).

2.2. Segunda Consigna: Capturando tráfico

Para capturar los mensajes ARP nuevamente utilizaremos la herramienta *scapy*: esta vez haremos uso de la función *sniff*, filtrando solamente los mensajes ARP. Para hacer luego un análisis de los datos obtenidos y poder comparar el comportamiento de distintas redes, tomamos los siguientes datos:

- `Captura Oficina`: Escuchamos durante aproximadamente ocho horas de una jornada laborable la red ethernet interna de una oficina de una empresa de software. Para cada paquete recibido guardamos todos los campos mencionados en la introducción, agregando el tiempo en el que se produjo la captura.
- `Captura Red ISP`: Escuchamos durante aproximadamente dieciséis horas (13:00 - 5:00) de un día hábil a través de un modem hogareño conectado directamente al ISP. Relevamos los mismos datos que para el caso anterior.
- `Captura Laboratorio`: Utilizamos además los archivos `pcap` provistos por la cátedra, correspondiente a capturas realizadas dentro de los laboratorios de la Facultad, con información de una red de alto tráfico ARP, y otra de poco tráfico (`big_arp.pcap` y `small_arp.pcap`). En este caso no contamos con información temporal.

[1] Si bien en condiciones normales, la asocicación IP-MAC debería ser única, en esta instancia consideramos que se pueden obtener múltiples respuestas. Para el análisis de los datos obtenidos en las secciones siguientes esto no será relevante pues sólo analizaremos relaciones entre direcciones IP

Una vez obtenidos los datos, analizamos la entropía de la red. Para ello definimos una fuente de información cuyos símbolos consisten en pares `<ip_fuente, ip_destino>`[2]. Estos símbolos son tomados de los mensajes ARP del tipo *who-has* que envía cada host[3]. Recordemos que los mensajes *is-at* se envían de manera privada al nodo que preguntó por esa IP, por lo tanto sólo podemos escuchar los del tipo *who-has*, o los *is-at* envíados a nuestra máquina. Para evitar considerar que la máquina que corre el sniffer es más sigificativa de lo que realmente es, sólo observaremos los paquetes *who-has*, dado que son los únicos mensajes que podemos ver en su totalidad. Con estas salvedades, consideramos que contamos con suficiente información, utilizando únicamente el protocolo ARP, para conocer y caracterizar la red en cuestión.

En estas condiciones, cada símbolo posible tiene una probabilidad de ocurrencia que se relaciona con la importancia del nodo dentro de la red: los nodos *significativos* (como, por ejemplo, el router) serán aquellos que aparezcan con mayor frecuencia en el campo `ip_destino`. La probabilidad de cada símbolo se calculará de manera empírica, en base a la cantidad de apariciones sobre el total de símbolos presentados (es decir, su frecuencia relativa). Además, podemos considerar que la fuente, definida de esta manera, es una fuente de memoria nula, ya que suponemos que los símbolos emitidos son estadísticamente independientes[4].

Una vez conseguidos los datos de captura, procesamos estos archivos con sus respectivos scripts en *Python*. Para todos los casos trazamos un grafo de red en base a los mensajes escuchados y calculamos la entropía total de la red. Esto lo realizamos trivialmente desde la definición, con la salvedad dicha anteriormente, de aproximar la probabilidad de ocurrencia de los símbolos por su frecuencia relativa. Para ajustar esta aproximación, consideramos períodos de tiempo prolongados. En los casos en que contábamos con información temporal sobre la captura de los paquetes, realizamos, además, el cálculo de la entropía para subintervalos disjuntos de una hora, de manera de observar la variabilidad de la red a lo largo del tiempo de captura. En todos los casos calculamos la entropía en bits, es decir, tomando logaritmo en base 2.

2.3. Tercera Consigna: Gráficos y Análisis

Para caracterizar una red buscamos, por un lado, encontrar los nodos relevantes de la misma. Contamos para esto con los símbolos mencionados en la sección anterior (pares `<ip_fuente, ip_destino>`), y con el valor de la información de cada nodo (en este caso, función de su frecuencia relativa), así como la entropía de la red[5]. A partir de estos datos podemos caracterizar cada una de las redes a estudiar observando la siguiente información:

1. Grafos dirigidos, en donde cada nodo representa una IP, y existe un eje desde el nodo A hasta el nodo B, si A hizo un pedido *who-has* a B (es decir, si el símbolo `<A, B>` apareció durante la captura). Dado que el trazado de aristas resulta imposible de interpretar a simple vista, lo simplificamos gráficamente, representando el grafo de manera circular y concéntrica, donde los nodos que se encuentran más al centro tienen mayor grado de entrada que los más distantes. No realizamos esto en un continuo, sino separándolo en clases en una escala logarítmica. Para no sobrecargar el gráfico no vamos a nombrar los distintos nodos; consideramos que la IP en particular con que se corresponden no es relevante.

2. Histograma relacionando cada IP con la cantidad de veces que fue consultada (es decir, que apareció en el campo `ip_destino`).

3. Cantidad de información de cada IP. En este caso puede compararse la información con la entropía total, y sacar conclusiones a partir de esto de cuáles son los nodos significativos. Cada barra representa un host distinto: nuevamente, no vamos a nombrar los distintos hosts por cuestiones de claridad del gráfico.

4. Entropía de la fuente en función de un rango horario. En este caso no estamos observando tanto los nodos significativos, sino cómo distintos tipos de redes pueden variar la cantidad de información presente según el momento del día, y el tipo de red que sea -hogareña, oficina, etc. Es de esperar que en un momento de mucha actividad de la red la variabilidad de los mensajes sea mayor, ya que las posibilidades de comunicación entre equipos aumenta considerablemente sólo por el hecho de que haya mayor cantidad de hosts conectados. Por otro lado, contrastaremos esta variabilidad con la entropía total calculada sobre toda la captura: si los valores correspondientes a subintervalos se corresponden con la entropía total, podremos deducir que la entropía de la red es relativamente constante, más allá del momento calculado, mientras que las discrepancias nos indicarán los períodos de mayor abundancia o escasez de información en la red.

[2] Consideramos los pares de manera ordenada, por lo cual no es lo mismo una combinación de IPs, que la misma combinación de manera invertida.

[3] El sniffer programado captura ambos tipos de mensaje ARP; al calcular la entropía filtramos primero los mensajes *who-has*.

[4] Esta suposición descarta casos patológicos, en los que, por ejemplo, la respuesta (o su ausencia) de un pedido pudiera generar nuevos, o bien tráfico intencionado más allá del normal funcionamiento del protocolo.

[5] Para caracterizar la red, consideramos que la asociación entre una IP y una dirección MAC no es relevante. Lo importante en este caso es la comunicación entre los distintos hosts, los cuales pueden representarse a través de su IP o de su dirección MAC. Elegimos utilizar la IP, pero podría haber sido cualquiera de las dos opciones.

5. Histograma de cantidad de apariciones de mensajes. Contamos cuántas veces aparece cada mensaje ARP, y graficamos en un histograma estas cantidades. Esto nos permite diferenciar la *variedad* de mensajes escuchados: la cantidad de observaciones de un mensaje es creciente de izquierda a derecha, con lo cual, un pico hacia la izquierda indicaría variedad de mensajes escuchados frecuentemente (pocas apariciones pero de muchos mensajes distintos), mientras que un equilibrio en el histograma indicaría que existe la misma abundancia de mensajes poco frecuentes que de usuales. Nos extenderemos al respecto en el análisis de los gráficos en concreto, relacionándolo con los valores de entropía medidos en subunidades de tiempo. Al igual que en el histograma anterior, cada barra representa un host, pero por cuestiones de claridad no se indica cuál es su IP específica.

3. Resultados

3.1. Implementación de un cliente ARP

De todos los casos mencionados en la sección 2.1, el único en que se recibió una respuesta con la dirección MAC solicitada es en el caso (1), es decir, al pedir direcciones MAC de nodos presentes dentro de la red local. En todos los otros casos el mensaje ARP no recibió respuesta alguna.

A través del uso de *Wireshark* pudimos observar con un poco más de detalle qué ocurrió en cada una de estas situaciones.

El caso (1) funcionó como se esperaba: al paquete *who-has* (enviado de manera broadcast) le sigue un paquete *is-at*, con el host cuya MAC se quiere conocer como origen, y dirigido únicamente a la máquina que preguntó.

Si se pregunta por una IP que no existe, pero que tiene una máscara correspondiente con la red local (por ejemplo, 192.168.0.2), no se observa ningún tipo de respuesta. Sin embargo, si se pregunta por un dirección cuya máscara no se corresponde con la red (casos 4, 6, 7, 8[6] y 9) se observa un intercambio de mensajes ligeramente diferente. En vez de enviar un paquete ARP de manera broadcast, la máquina pregunta primero quién tiene la dirección (en nuestro caso) 192.168.0.1 (dirección del router). Al recibir la respuesta *is-at* con la MAC correspondiente, pregunta específicamente al router quién tiene la dirección buscada. Es decir, pareciera ser que antes de enviar mensajes ARP, automáticamente se calcula si dicha IP se encuentra dentro de la red local. Si no se encuentra, se ejecuta el intercambio mencionado, enviando el pedido por la IP buscada directamente al router (del cual no se recibe respuesta, al menos en los casos probados).

3.2. Captura de tráfico

Como mencionamos, se escucharon durante varias horas distintos tipos de redes. A partir de los datos obtenidos calculamos la entropía de la manera explicada en la sección anterior. Los resultados obtenidos fueron los siguientes:

Captura de cátedra: big_arp.pcap	7.057
Captura de cátedra: small_arp.pcap	6.227
Red hogareña	6.749
Red de oficina	7.428

A continuación se muestran los gráficos generados a partir de los datos obtenidos en esta sección.

[6] En el caso de una direccón inválida, la dirección enviada se traduce a una dirección IP correcta (en este caso se envió el paquete preguntándo por la dirección 7.91.205.21).

3.2.1. Grafos

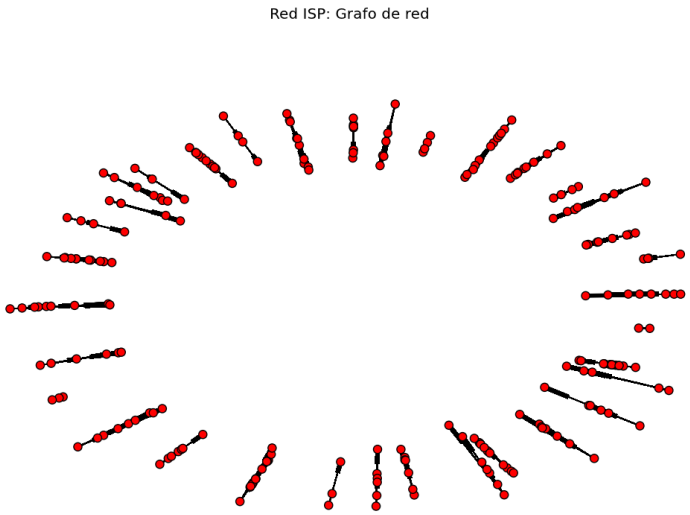


Figura 1: Grafo de IPs - Red ISP

Lo más notable de la figura 1, como se verá en contraste con las siguientes, es que presenta numerosas componentes conexas pequeñas. Atribuimos esta disposición a que, dado que corresponde con una red de ISP, la interacción, en principio, no se da entre cualqueir par de nodos por igual, ya que obedece a motivos *personales* de los usuarios. De todas formas, la inconexión da la idea de que no existe un nodo centralizador a través del cual se canalice el tráfico (típicamente un router), con lo cual el funcionamiento de la red sería imposible. Por lo tanto, suponemos que, por razones del proveedor, esa información no se transmite via ARP (puede utilizar otros protocolos), o se controla el tráfico de paquetes ARP con destinos sensibles para la red.

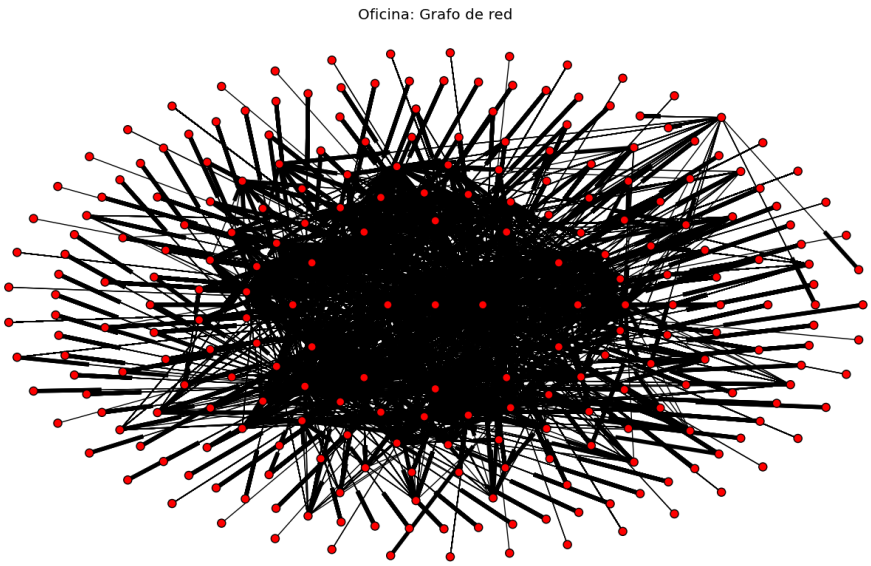


Figura 2: Grafo de IPs - Oficina

En el caso de la figura 2, observamos todo lo contrario. Recordemos que los nodos ubicados más al centro corresponden con las direcciones más solicitadas, típicamente routers/gateways. El alto grado de conexión entre los nodos

centrales refleja la intensa actividad que ocurre entre los hosts en una red privada (ej: clientes de chat). También se observan nodos en el círculo exterior que, no sólo realizan pocas consultas ARP, sino que también nunca le son respondidas. Estos pueden ser dispositivos que se conectaron por poco tiempo y para realizar una tarea espefícica, o direcciones inválidas que no fueron consideradas por el resto de la red para recibir datos.

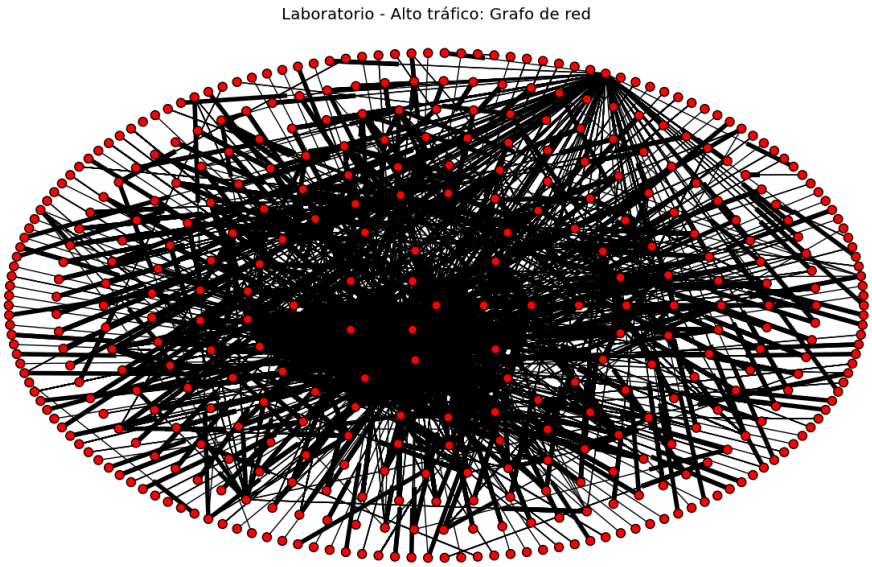


Figura 3: Grafo de IPs - big_arp.pcap

Para el grafo de la figura 3, se observa algo similar que en la figura 2. Pocos nodos con un alto nivel de solicitudes, y una disposición numerosa a su alrededor. Cabe el mismo análisis que en el caso anterior, destacando también la presencia de un nodo del círculo exterior que realiza numerosos pedidos, pero que no le son respondidos en la misma medida. Nuevamente, atribuimos este hecho a la presencia de direcciones anómalas (por ejemplo, 0.0.0.0).

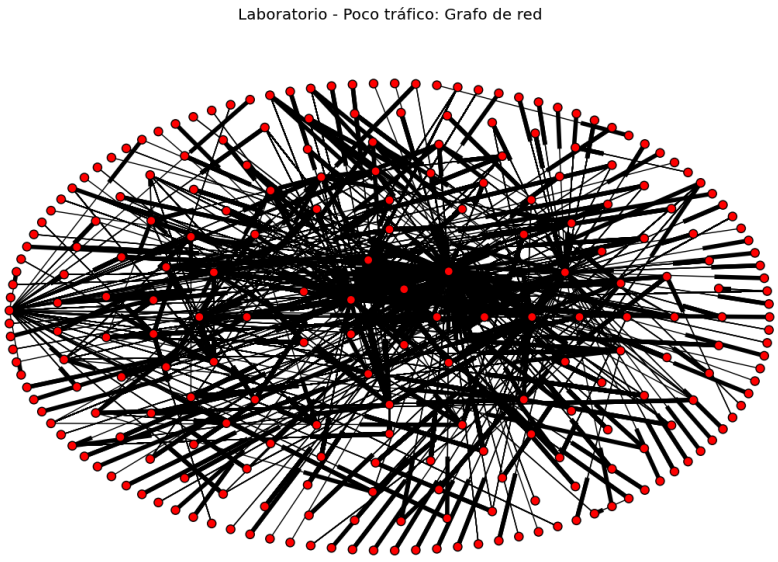
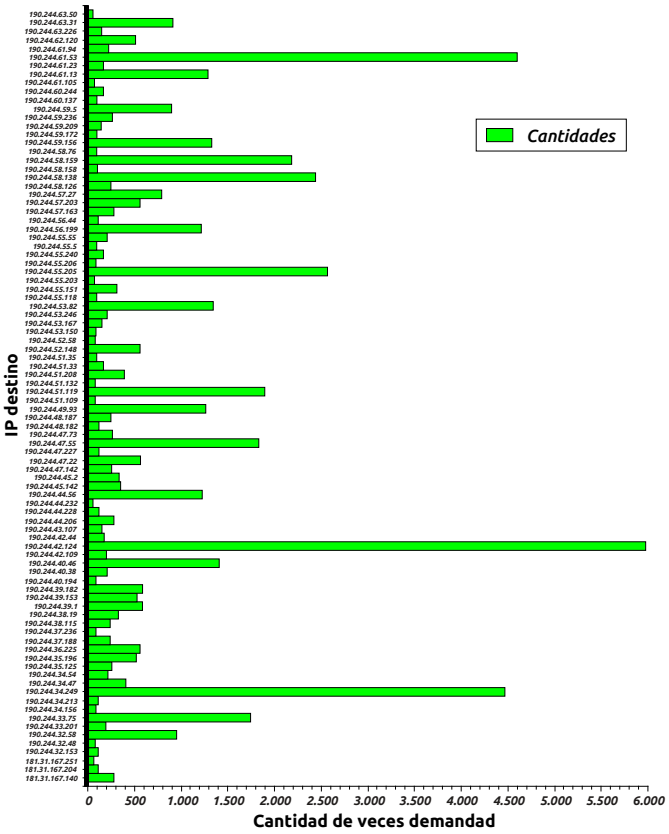


Figura 4: Grafo de IPs - small_arp.pcap

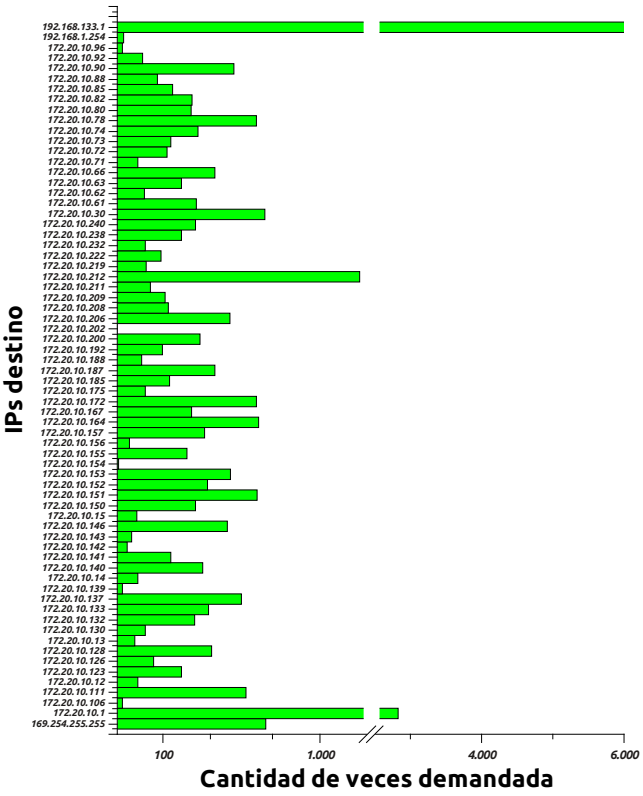
Por último, en la figura 4 vemos nuevamente un esquema similar a los anteriores, pero con mejor detalle, ya que

el nivel de tráfico es menor. Igualmente existen las direcciones anómalas y los nodos distinguidos en el centro, pero se puede apreciar mejor el intercambio entre los nodos menos distinguidos de la red.

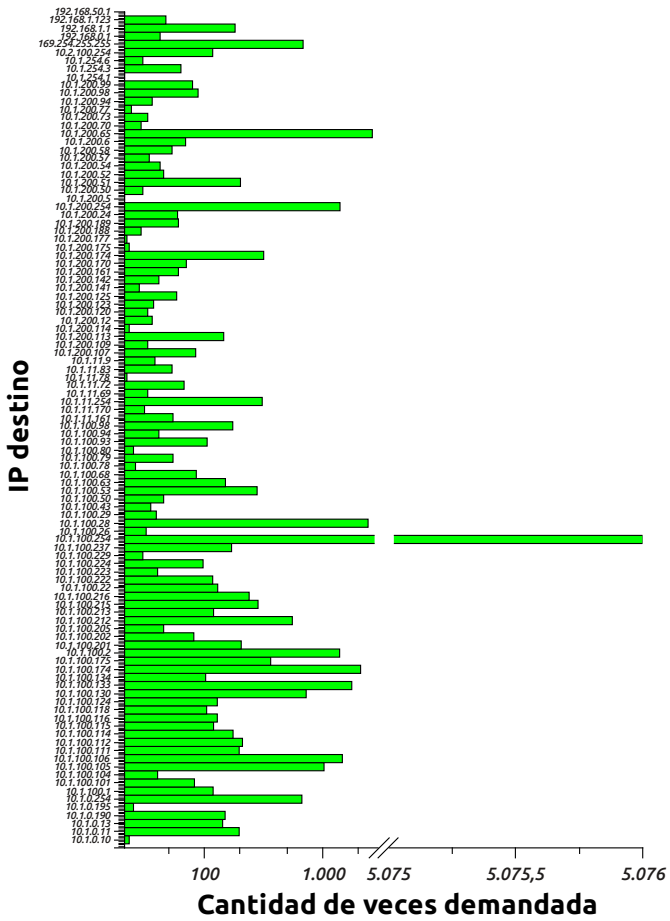
3.2.2. Gráficos de demanda



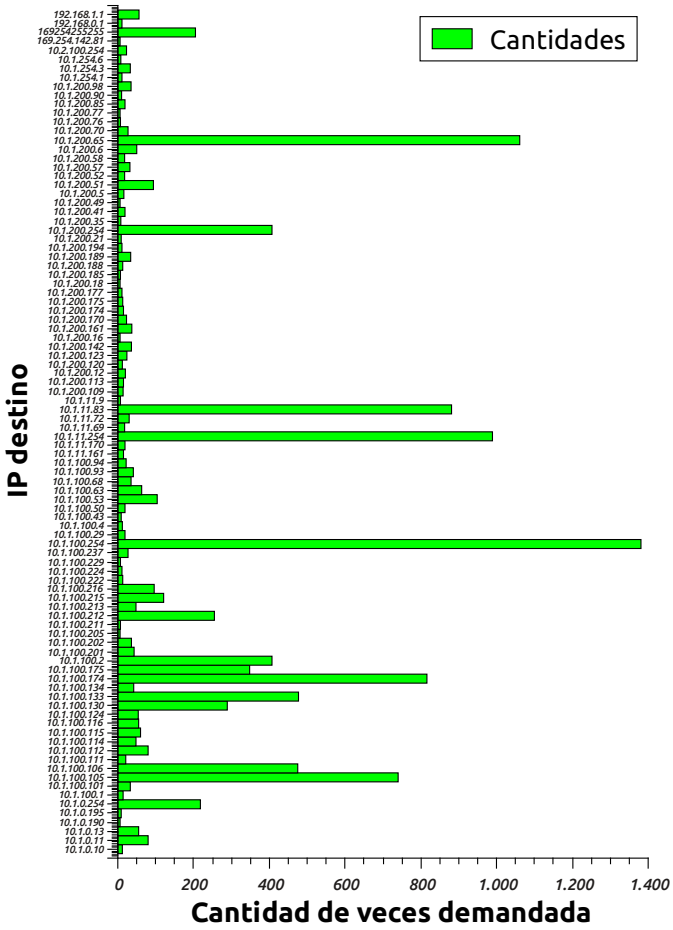
(a) Cantidad de demandas a cada IP - Red ISP



(b) Cantidad de demandas a cada IP - Oficina



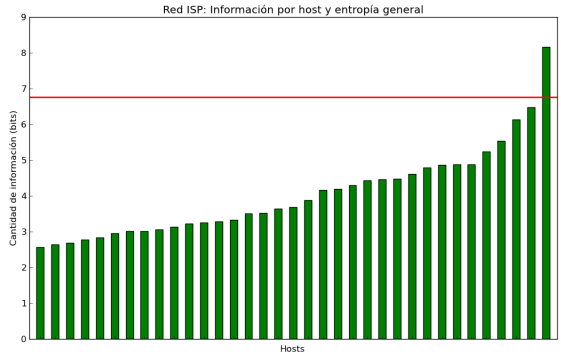
(c) Cantidad de demandas a cada IP - big_arp.pcap



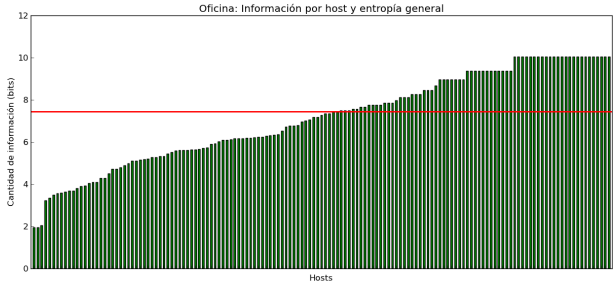
(d) Cantidad de demandas a cada IP - small_arp.pcap

Las figuras 5a, 5b, 5c, 5d nos dan una idea de la distribución de los nodos significativos en cada una de las redes estudiadas: en todos los casos, unos pocos concentran la mayoría de los pedidos. Se aprecia claramente en estos gráficos cuáles son las IPs más solicitadas, que asociamos con nodos funcionalmente significativos en la red (servidores, routers, etc).

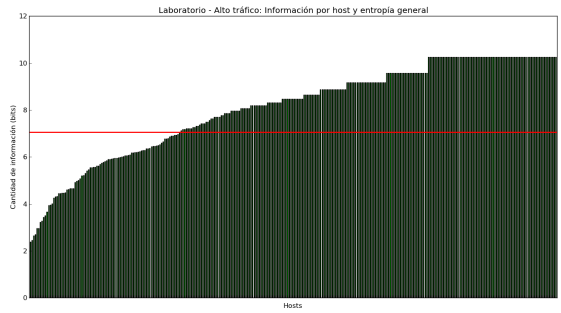
3.2.3. Información de los nodos



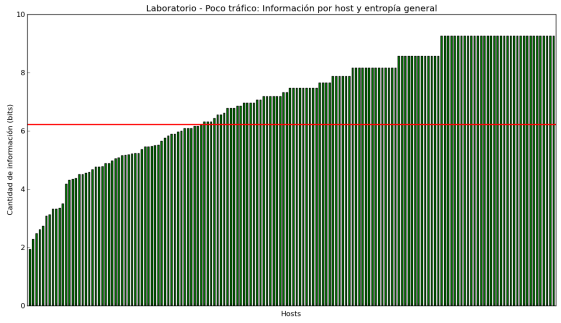
(e) Cantidad de información según host - Red ISP



(f) Cantidad de información según host - Oficina



(g) Cantidad de información según host - big_arp.pcap

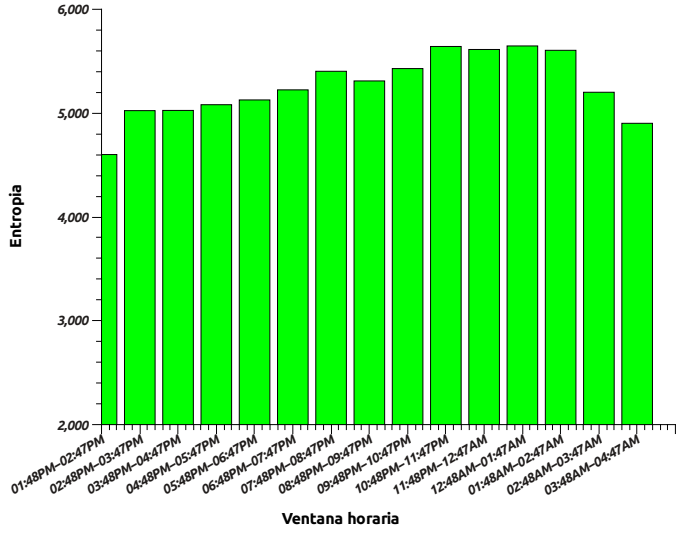


(h) Cantidad de información según host - small_arp.pcap

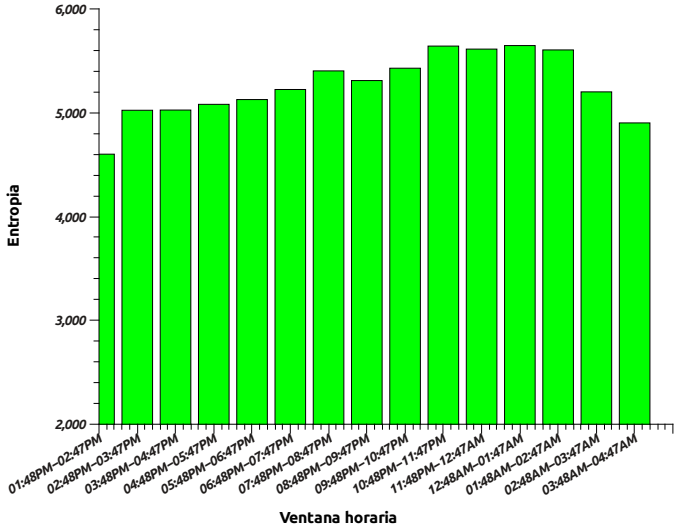
En las figuras 5e, 5f, 5g, 5h distinguimos los nodos de una manera diferente: graficamos la cantidad de información para cada host, superponiendo la entropía medida (línea roja). En los casos correspondientes a los laboratorios (figuras 5g y 5h), observamos una importante proporción de nodos que aportan más información que la media. Asociamos esto con los nodos poco consultados que observábamos en los grafos anteriores. Para la figura 5f observamos una proporción más pareja, pero vale el mismo comentario.

En la figura 5e podemos observar que solamente uno de los nodos supera la entropía. Asociamos esto con el hecho de que la red presenta varias componentes conexas: no existen nodos particularmente significativos, sino que, por la topología de la misma, muchos cumplen este papel.

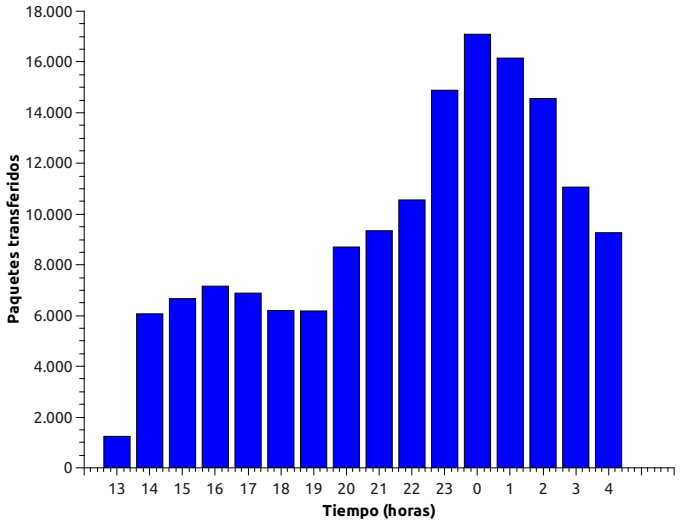
3.2.4. Mediciones en función del tiempo



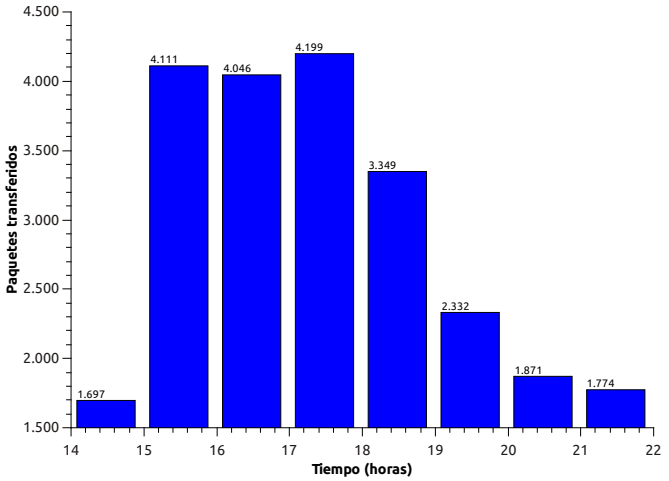
(i) Entropía en función de la franja horaria - Red ISP *** FALTA!



(j) Entropía en función de la franja horaria - Oficina



(k) Cantidad de paquetes enviados en función de la franja horaria - Red ISP



(l) Cantidad de paquetes enviados en función de la franja horaria - Oficina

De las figuras 5k y 5l podemos deducir dos comportamientos diferentes de la red, mirando su evolución a lo largo del tiempo. Si comparamos los valores obtenidos en la figura correspondiente a la ISP, con la entropía medida, vemos que si bien no la alcanza, no presenta una variabilidad significativa a lo largo del tiempo (más allá de la atribuible al aumento de tráfico que puede haber en las horas de la tarde-noche). Lo contrario sucede para la red de la oficina: el pico de entropía medida coincide con la cantidad de paquetes enviados durante un horario de intensa actividad, llegando incluso a superar la entropía en forma general. Observamos que con el correr de las horas esta situación se revierte completamente. Esto indica que la información que proveen a la red los mensajes ARP a lo largo de la tarde proviene mayormente de un rango horario más acotado, pasado el cual, baja enormemente. Atribuimos este hecho a que permanecen encendidas sólo algunas computadoras de las que se comunicaban antes, con lo cual los mensajes generados en este período no aportan a la cantidad de información diaria de la red, pues ya fueron observados anteriormente. Al ser menor el volumen de actividad, es de esperar que la variabilidad de comportamiento de los hosts sea menor, con lo cual los pedidos tienden a regularizarse, y por ende, aportan menos información. Esta disminución en la variabilidad de comportamiento no se observa en la red ISP, ya que dada la magnitud de la red (y, es posible, alguna estrategia de optimización por parte del proveedor) sigue siendo lo suficientemente general y diversa, tanto en períodos de baja como de alta actividad.

3.2.5. Histogramas de frecuencia

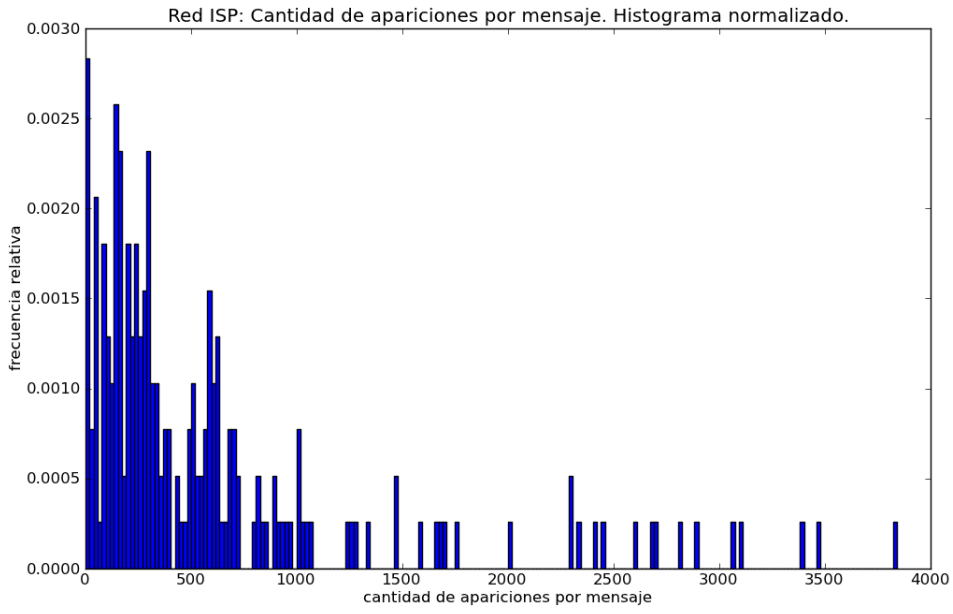


Figura 5: Cantidad de apariciones de cada mensaje ARP - Red ISP

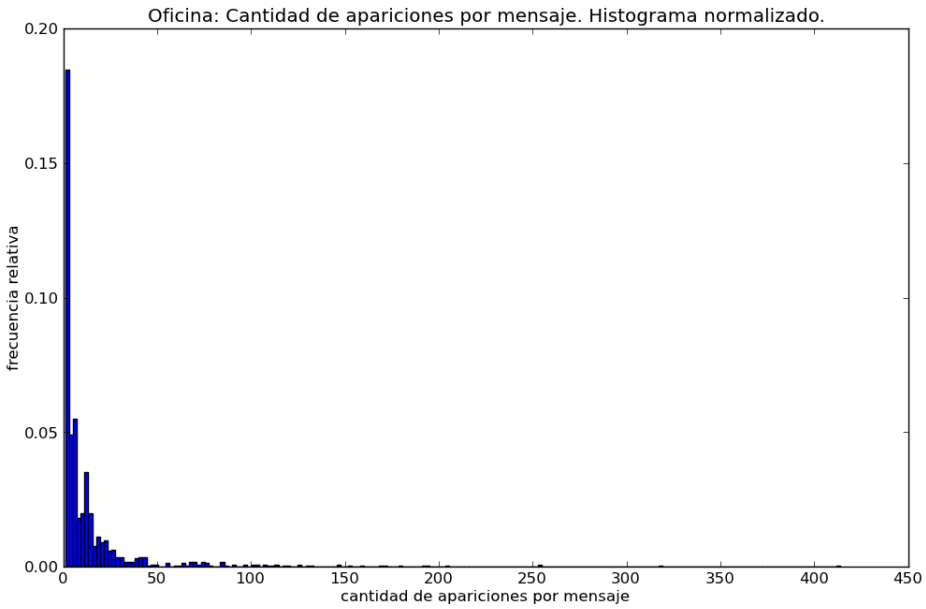


Figura 6: Cantidad de apariciones de cada mensaje ARP - Oficina

Como adelantamos anteriormente, en las figuras 5 y 6 comparamos los histogramas de repetición de mensajes para la red Oficina y la ISP. Estos histogramas refuerzan la idea explicada anteriormente: para el caso del ISP, se observa una uniformidad mayor, que puede corresponderse con la variabilidad sostenida. Para la red de Oficina, por otro lado, puede observarse, además de la abundancia de paquetes con pocas apariciones (hecho común en ambos casos, atribuible a mensajes erróneos o dispositivos específicos de poca actividad), un decaimiento muy rápido en la cantidad de apariciones, que no se recupera. Esto es consistente con el comentario sobre la dinámica de funcionamiento de la oficina comentada: sólo un subconjunto de los hosts permanece operativo suficiente tiempo de la muestra, y éstos son los que extienden el histograma hacia la derecha. Los restantes, son los abundantes y poco frecuentes que contribuyen a elevar la entropía al pico máximo, y en definitiva, son los que más aporte realizan a la hora de calcular la información media durante la jornada. Justamente, para el caso de la ISP, se ve que esta responsabilidad está más compartida (el histograma decae más lentamente) y la parte significativa se extiende más.

4. Conclusiones

Habiendo hecho la presentación de los resultados y sus comentarios específicos pertinentes, quedan para esta sección los comentarios generales sobre la experiencia realizada. Por un lado, vale destacar la posibilidad de conocer una red y su comportamiento observando únicamente mensajes de protocolos de capa de enlace, sin tener en cuenta los datos transmitidos por las capas superiores: con el análisis de los grafos de red vimos cómo se pueden diferenciar esquemas muy distintos (red privada vs. red pública), y dentro de las privadas, nodos y comportamientos particulares: nodos centralizadores (que podemos identificar con routers) y comportamientos anómalos (multiplicidad de solicitudes y ninguna respuesta, o una única solicitud y ninguna respuesta). Además, pudimos observar una situación muy poco esperable en el caso de la red pública, para la cual no podemos, en principio, establecer una respuesta. En cualquier caso, obliga a pensar que las redes públicas, por su importancia y alcance, son manejadas con una complejidad mayor; para comprenderlas se necesitaría observar más de lo que puede aportar el uso del protocolo ARP.

Por otro lado no resulta menos interesante observar empíricamente las abstracciones propuestas por la teoría de la información, y cómo esta generaliza situaciones diversas, que también terminan por caracterizar a la red. Más allá de los valores de entropía obtenidos, sobre los cuales no pretendemos opinar cuantitativamente, y que podemos considerar próximos entre sí, resulta interesante los casos en que podemos diferenciar por tiempos, y nuevamente, caracterizar a las redes de las que provienen, teniendo en cuenta únicamente la interacción entre las computadoras y no el contenido o la razón de esta comunicación. Insistimos con el contraste entre la red ISP y la situación de oficina, ya que es un buen ejemplo de lo que se considera *información* dentro de la teoría: no se trata (sólamente) de la presencia de mensajes, sino también de sus particularidades propias y generales: mientras que la primera debe su cantidad de información a la constante presencia de nodos diversos y una interacción moderada, la segunda es producto de una intensa interacción, donde parecería que se agotan las posibilidades, dejando a las horas siguientes repeticiones de un subconjunto de

mensajes, hecho que, no sorprendentemente, no aporta grandes cantidades de información.

Para concluir, en el presente TP observamos distintas redes, utilizando por un lado un elemento puramente técnico (la relación entre direcciones IPs para deducir interacciones y distinguir participantes) y por otro, uno puramente teórico (adaptado para su cálculo efectivo) con el que podemos medir cuán relevante o no son las interacciones anteriormente detectadas, indicios suficientes para realizar caracterizaciones con sólo escuchar el mensajeo protocolar.