TP1: Wiretapping

GRUPO 9: Adrián Bonaccini, Natalia Enrique, Julián Len, Nicolás Len

Departamento de Computación
FCEyN - UBA

9.10.2017

Resumen

El siguiente trabajo tiene como objetivo analizar diferentes redes a través de distintas formas de modelado basándonos en conceptos de teoría de la información. Se intentará estudiar, a través de la entropía y la información de sus símbolos, las fuentes modeladas para poder encontrar nodos distinguidos y entender a grandes rasgos la configuración de sus topologías.

I. Introducción

En el siguiente trabajo se realizaron capturas de cuatro redes de distinta configuración y se definieron dos fuentes de información detalladas a continuación y sometidas a distintos análisis.

- Fuente S_1:
  En este caso, la fuente fue provista por la cátedra. Los símbolos de la misma están formados por la combinación entre el tipo de destino de la trama (broadcast o unicast) y el protocolo de la capa inmediata superior.

- Fuente S_2:
  En este caso, se nos propone modelar una fuente S_2 con el objetivo de distinguir los nodos de la red utilizando únicamente las direcciones IP dentro de los paquetes ARP.
  La fuente propuesta está compuesta por las direcciones IP tales que en el paquete ARP, al enviar un mensaje WHO-HAS, son destino.
  Es decir, cada vez que se envíe un paquete a la red local preguntando por la MAC asociada a una IP, esta dirección será considerada un símbolo de nuestra fuente.

II. Desarrollo de la Herramienta

- Fuente S_1:
  Para el desarrollo de la herramienta de la fuente S_1, utilizamos el campo **type** del paquete que nos brinda el protocolo que se está utilizando. Luego, dentro del mismo paquete, utilizando el campo dst chequeamos si se trata de un mensaje de tipo broadcast (ff:ff:ff:ff:ff:ff) o unicast (cualquier otro). Una vez distinguidos los símbolos de la fuente, los guardamos en un diccionario con el objetivo de tener para cada símbolo, la cantidad de apariciones en la fuente.

- Fuente S_2:
  La funcionalidad de la herramienta en este caso será la misma. Nos basamos en un diccionario, en el cual para cada símbolo de la red tendremos su cantidad de apariciones.
  Para distinguir los símbolos de la misma, primero filtramos los paquetes por ARP, luego en su campo **op** distinguimos si son de tipo WHO-HAS. Finalmente, nos quedamos con el campo destino del paquete, la dirección IP.

III. Muestras

Para la experimentación se tomaron capturas de las redes detalladas a continuación:

- Red Hogareña
- Laboratorios DC
- Biblioteca Noriega
- Starbucks

Para cada una de ellas se tomaron aproximadamente 30000 paquetes que serán estudiados en la sección siguiente. En principio, dado que tres de las redes son abiertas, desconocemos la topología de las mismas y la

cantidad de dispositivos conectados simultáneamente. Caso contrario es el de la Red Hogareña, ya que la medición se realizo con 5 dispositivos conectados a la red, todos utilizando Internet (llamadas de **Skype**, **YouTube**, **WhatsApp**).

IV. Resultados de Experimentación

1. Red Hogareña

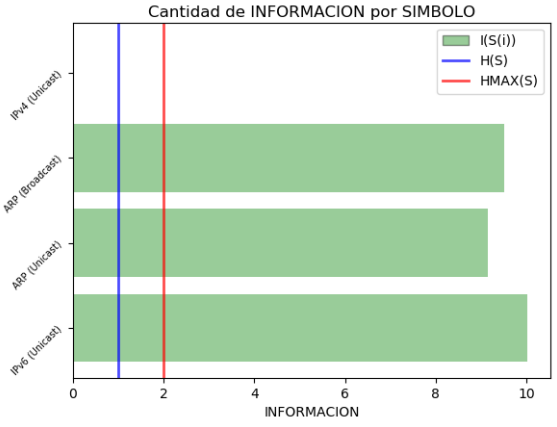
1.1. Fuente S_1

Luego de obtener la captura de esta red, se analizó el tráfico bajo el modelo referido como fuente S_1, en donde podremos distinguir los protocolos utilizados en la red durante la captura y si son broadcast o unicast.

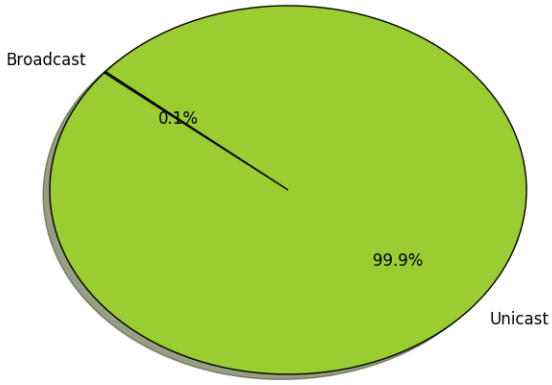
La herramienta arrojó los siguientes resultados:

Cuadro 1: *Red Hogareña, info. por símbolo*

Datos fuente S_1		
SIMBOLO	P(s_i)	I(s_i)
(Unicast, IPv4)	0.996	0.006
(Unicast, ARP)	0.002	9.143
(Broadcast, ARP)	0.001	9.518
(Unicast, IPv6)	0.001	10.027
H(S_1) = 1 (0.04)		
$H_{max}(S_1)$ = 2 (2.00)		



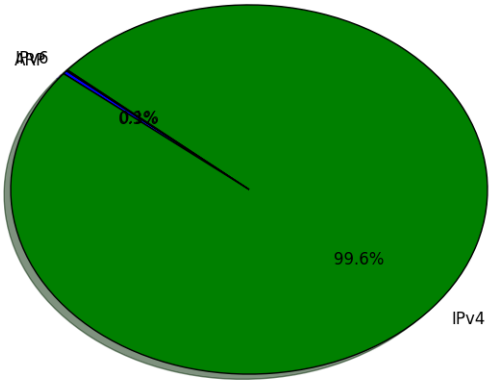
Nuestra hipótesis de trabajo vincula el tamaño de la red (en cantidad de hosts, tramas) respecto de la entropía de la fuente, por ende esperábamos un valor bajo. Sin embargo, la misma no se aleja demasiado de la máxima que es la que se obtiene en condiciones de equiprobabilidad.



Podemos notar que el porcentaje tráfico broadcast es muy bajo, esto puede deberse a que la red es pequeña y todos los dispositivos son conocidos por la misma.

Se encontraron los siguientes protocolos:

- ARP: Éste es un protocolo de control ya que se ocupa de encontrar la MAC que correspone a una dirección IP.
- IPv4 y IPv6: Éstos transportan datos de un nodo fuente hacia uno destino. La principal diferencia entre IPv4 y IPv6 es que la primera tiene direcciones de 32 bits, mientras que la segunda de 128 bits.



Observando el gráfico de la informacion de la fuente, y basándonos en teoría de la información, podemos decir que cuando un símbolo tiene alta probabilidades, es decir que su aparición es alta en dicha fuente, la información del mismo será baja. Más aún, cuando la información de un símbolo se encuentra por debajo de la entropía de la fuente, el mismo será distinguido.

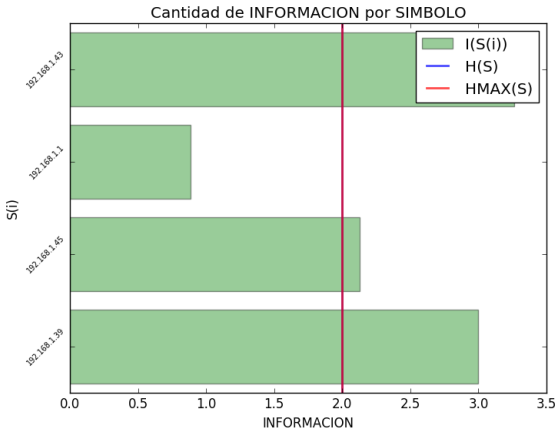
En este caso, dicho símbolo es $(Unicast, IPv4)$. Como mencionamos en sección de Muestras, en esta captura se utilizó **YouTube**, **WhatsApp** y **Skype** entre los dispositivos, por esta razón es que el protocolo IPv4 será el distinguido, ya que se estuvo transmitiendo datos.

i.2. Fuente S_2

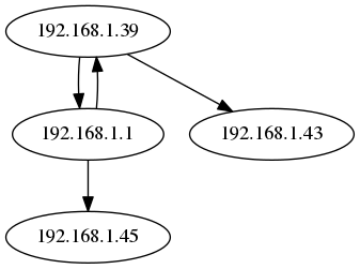
Reformando la herramienta para la fuente propuesta se obtuvo la siguiente tabla:

Cuadro 2: *Red Hogareña, info. por símbolo*

Datos Fuente S_2		
IP	P(s_i)	I(s_i)
192.168.1.1	0.542	0.885
192.168.1.45	0.229	2.126
192.168.1.39	0.125	3.0
192.168.1.43	0.104	3.263
H(S_2) = 2 (1.68)		
$H_{max}(S_2)$ = 2 (2.00)		



Nuevamente, los resultados arrojados nos indican que la entropía de la fuente es distinta de la máxima, aunque no difieren demasiado, esto puede deberse al tamaño de la red en la que se realizó la muestra. Para la distinción de símbolos, utilizaremos el mismo criterio que para la fuente S_1, en este caso aquellos símbolos que están por debajo de la entropía serán los distinguidos pero representarán aquellas direcciones para las cuales se hicieron más pedidos ARP, de esta forma, podríamos encontrar aquellas direcciones IP que representan el **default gateway** de la red. Podemos notar que en este caso, nuestro símbolo distinguido será **192.168.1.1**, que efectivamente es el router del hogar. Por último, podemos ver un grafo con la topología de la red.



Podemos observar nuestro símbolo distinguido que es aquel con el que más se intercambian mensajes, además las IP **192.168.1.39** y **192.168.1.43** corresponden a la computadora en donde se realizó el experimento y una tablet respectivamente, en donde se estaba realizando una llamada de **Skype**. Como ambos dispositivos pertenecen a la red y ya son conocidos interactúan entre ellos, sin que **192.168.1.43** tenga que comunicarse con el router.

II. Laboratorios DC

Para la siguiente red, se analizó el tráfico bajo el modelo referido como fuente S_1 en donde pudimos distinguir ciertos protocolos utilizados en la red durante el tiempo de captura, además de si las tramas eran broadcast o unicast. También se analizó bajo el modelo de la fuente S_2, obteniendo distintas IP.

La muestra fue tomada con la red WiFi de los laboratorios del Departamento de Computación, un día Viernes a la tarde. La red se compone de un router WiFi abierto al público por lo que se espera distinguir la IP del router, y que el resto de las IP tengan una probabilidad parecida.

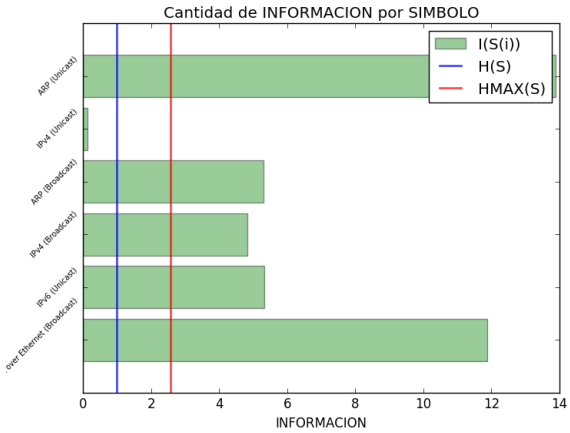
II.1. Fuente S_1

Para la fuente S1, el resultado del análisis del tráfico fue el siguiente:

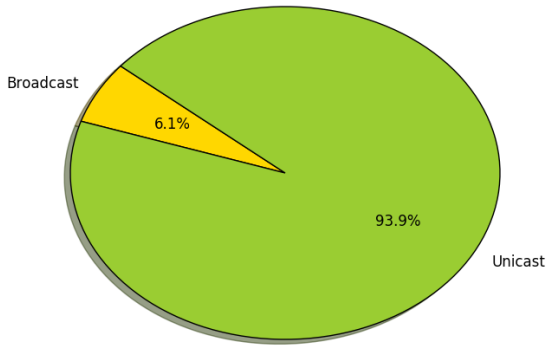
Cuadro 3: *Laboratorio DC, info. por símbolo*

Datos fuente S_1		
TIPO	P(s_i)	I(s_i)
(Unicast, IPv4)	0.914	0.129
(Broadcast, IPv4)	0.035	4.833
(Broadcast, ARP)	0.025	5.299
(Unicast, IPv6)	0.025	5.336
(Broadcast, ATA)	0.0	11.887
(Unicast, ARP)	0.0	13.887
H(S_1) = 1 (0.56)		
H_{max}(S_1) = 3 (2.58)		

Se esperaba que la entropía de la fuente no sea máxima, pues es casi imposible que la fuente sea equiprobable, ya que por cada maquina que se conecta a la red, se mandan ARP's y también constantemente hay envío de datos con IPv4/IPv6. Como se puede ver en la tabla anterior y como era esperado, la entropía es menor que la entropía máxima.



En el resultado, se destacan distintas tramas Unicast y Broadcast, con una predominancia de las Unicast de protocolo IPv4. Esto se puede deber a que el router y los hosts se conocen entre si y en general el tráfico que se presenta en la red es de información desde y hacia Internet. El porcentaje preciso se puede ver en el siguiente gráfico,



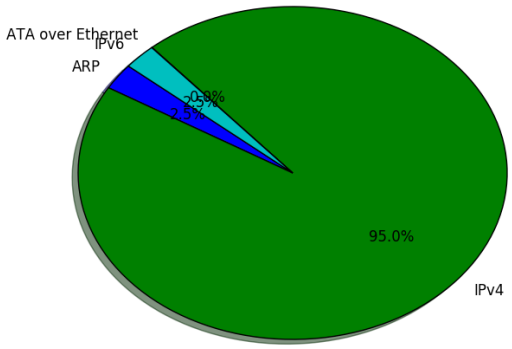
Luego, las funciones de los distintos protocolos encontrados fueron:

- ARP.
- IPv4 y IPv6.
- ATA: Éste es un protocolo de red diseñado para acceder a dispositivos de almacenamiento ATA mediante redes Ethernet. Proporciona la posibilidad de construir redes de almacenamiento de bajo costo con tecnologías estándar.

Observando el gráfico de la informacion de la fuen-

te, y basándonos en teoría de la información, podemos decir que cuando un símbolo tiene alta probabilidades, es decir que su aparición es alta en dicha fuente, la información del mismo será baja. Más aún, cuando la información de un símbolo se encuentra por debajo de la entropía de la fuente, el mismo será distinguido.

En este caso, dicho símbolo es $(Unicast, IPv4)$.



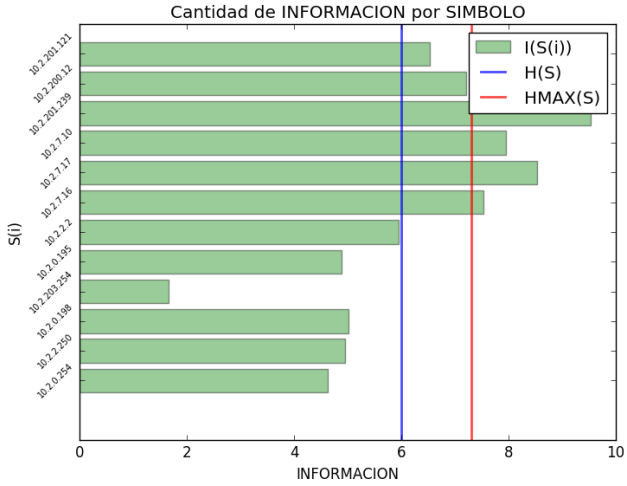
Al igual que en el experimento anterior, podemos decir que en general, se usan servicios como sitios web de materias, aplicaciones como **WhatsApp**, etc, y por esta razón es que el protocolo IPv4 será el distinguido, ya que lo que producen principalmente es que se transmitan datos constantemente.

ii.2. Fuente S_2

Luego en la fuente S2, los resultados del análisis fueron:

Cuadro 4: *Laboratorio DC, info. por símbolo*

Datos fuente S_2		
IP	P(s_i)	I(s_i)
10.2.203.254	0.317	1.659
10.2.0.254	0.04	4.628
10.2.0.195	0.034	4.891
10.2.2.250	0.032	4.95
10.2.0.64	0.031	5.012
	...	
10.2.1.14	0.001	9.535
H(S_2) = 6 (5.28)		
$H_{max}(S_2)$ = 8 (7.30)		



Al igual que en S_1, la entropía de la fuente S_2 no es máxima. Esto se puede deber que al ser una red abierta, existen host que se conectan por un tiempo acotado. Esto genera que en la red hayan host desconocidos y en las tramas ARP aparezcan ciertas IP nuevas constantemente.

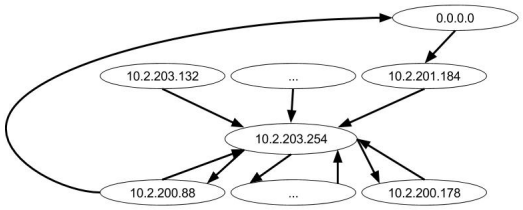
Basándonos en el criterio utilizado en los experimentos anteriores tomaremos como símbolos distinguidos aquellos que se encuentran por debajo de la entropía.

En el gráfico podemos notar que 6 de ellos están por debajo pero nótese que hay una de ellas (10.2.203.254) que se diferencia delresto, ya que la información que provee es más pequeña. Podemos suponer que esta dirección corresponde al default gateway de la red. Para el resto de los símbolos distinguidos en principio no podemos asegurar nada, si bien no se sabe con presición cómo esta compuesta la red del Departamento, sabemos que la misma es una red compleja en comparación con otras estudiadas en este trabajo, por lo tanto dichas direcciones bien podrían pertenecer a dispositivos que cumplen una función clave en la red los cuales desconocemos.

A la hora de graficar la topología de la red, nos encontramos con distintas subredes separadas que no se comunicaban entre ellas. Tomamos la desición de graficar aquella subred que era más grande y predominaba en aristas y nodos. Además, notamos que en las otras, la comunicación no tenia respuesta, lo que no sucede con la que escogimos graficar. Es de-

cir, que en la escogida, tenemos nodos que envían un mensaje arp y es contestado, mientas que en las otras no sucede. Esto nos podría indicar que el host ditingido sí pertenecía al router de la red, mientas que las otras subredes ya se conocían entre sí y no necesitaban comunicación con el mismo.

Finalmente presentamos un modelo resumido con los nodos y comunicaciones más importantes de la red. Se dejaron aquellos nodos para los cuales teniamos más entradas y salidas.



Podemos ver lo desarrolado anteriormente, las direcciones que envían y reciben respuesta de nuestro host destacado.

Además notamos la aparición de la dirección 0.0.0.0 la cual representa la "dirección por defecto.[en] las tablas de ruteo.

III. Biblioteca Noriega

Para la siguiente red, se analizó el tráfico bajo el modelo referido como fuente S_1 en donde pudimos distinguir ciertos protocolos utilizados en la red durante el tiempo de captura, además de si las tramas eran broadcast o unicast. También se analizó bajo el modelo de la fuente S_2, obteniendo distintas IP.

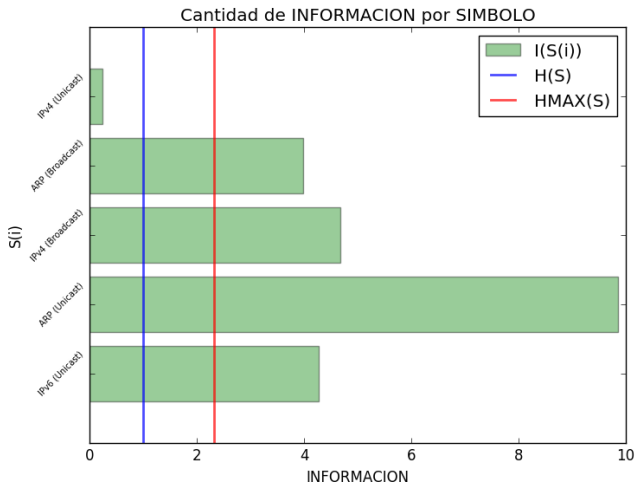
La muestra fue tomada en la Biblioteca Noriega, un día Viernes a la tarde. La red se compone de un router WiFi abierto al público por lo que se espera distinguir una IP en particular (la del router), y que el resto de IP tengan una probabilidad parecida.

Luego, para la fuente S1, el resultado del análisis del tráfico fue el siguiente,

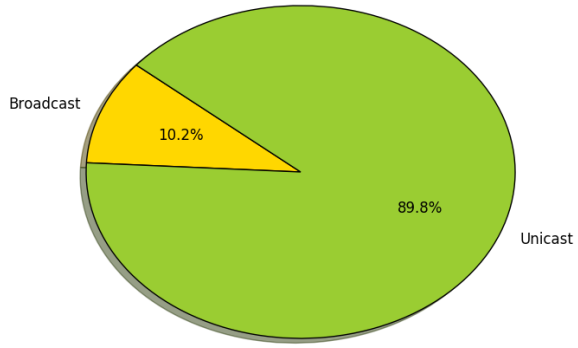
III.1. Fuente S_1

Cuadro 5: *Biblioteca Noriega, info. por símbolo*

Datos fuente S_1		
TIPO	P(s_i)	I(s_i)
(Unicast, IPv4)	0.845	0.243
(Broadcast, IPv4)	0.039	4.68
(Broadcast, ARP)	0.063	3.982
(Unicast, IPv6)	0.052	4.272
(Unicast, ARP)	0.001	9.854
H(S_1) = 1 (0.87)		
$H_{max}(S_1)$ = 3 (2.32)		



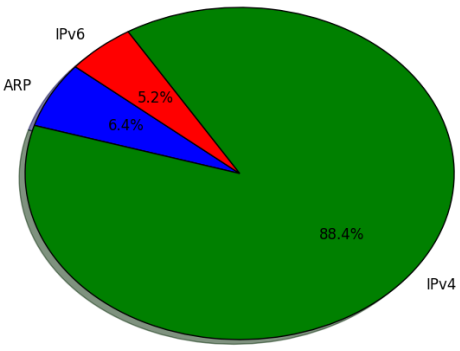
En el resultado, se destacan distintas tramas Unicast y Broadcast, con una predominancia de las Unicast. Esta particularidad, se puede deber a que el tráfico en general de la red, es saliente, y los host ya conocen la ubicación del router. El porcentaje preciso se puede ver en el siguiente gráfico,



Luego, las funciones de los distintos protocolos encontrados fueron:

- ARP.
- IPv4 y IPv6.

Observando el gráfico de la informacion de la fuente, y basándonos en teoría de la información, podemos decir que cuando un símbolo tiene alta probabilidades, es decir que su aparición es alta en dicha fuente, la información del mismo será baja. Más aún, cuando la información de un símbolo se encuentra por debajo de la entropía de la fuente, el mismo será distinguido. En este caso, dicho símbolo es $(Unicast, IPv4)$.



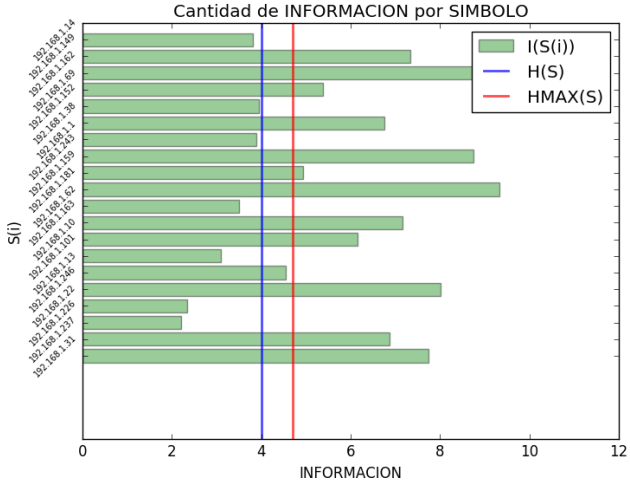
Como mencionamos en el experimento de la red hogareña, en un ambiente como la Biblioteca, en general, se usan servicios como YouTube, Whatsapp, páginas web de materias, y por esta razón es que el protocolo IPv4 será el distinguido, ya que se estuvo transmitiendo datos.

iii.2. Fuente S_2

Luego en la fuente S2, los resultados del análisis fueron

Cuadro 6: *Biblioteca Noriega, info. por símbolo*

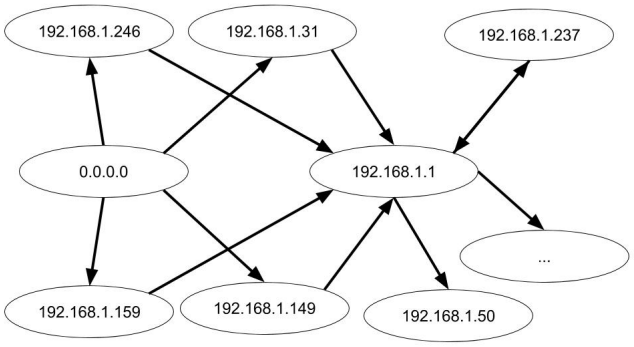
Datos fuente S_2		
IP	P(s_i)	I(s_i)
192.168.1.226	0.217	2.207
192.168.1.22	0.198	2.337
192.168.1.101	0.117	3.093
192.168.1.62	0.089	3.498
192.168.1.14	0.071	3.807
192.168.1.1	0.068	3.888
	...	
192.168.1.162	0.001	10.331
H(S_2) = 4 (3.45)		
$H_{max}(S_2)$ = 5 (4.70)		



Como primer comparación a tener en cuenta, la entropía de la fuente S_2 no es máxima. Esto quiere decir, que no hay equiprobabilidad entre las distintas IP. Esto puede ser por distintos motivos, entre ellos, al ser una red abierta existen host que se conectan por un tiempo acotado. Esto genera que en la red hayan host desconocidos y en las tramas ARP aparezcan

ciertas IP nuevas constantemente. En caso de ser una red con pocos nodos, es más probable que la entropía sea máxima ya que en el tráfico las IP generalmente serían las mismas y ya serían conocidas.

Los nodos distinguidos que elegimos fueron, el **192.168.1.226**, **192.168.1.22** y el **192.168.1.1**. Los primeros dos ya que su información esta muy por debajo de la entropía. Creemos que esto se debe, a que son nodos que hacen uso intensivo de la red, como por ejemplo PCs fijas de la biblioteca. Mientras que la **192.168.1.1** creemos que es conveniente distinguirla dada la siguiente topologías



Antes de explicar la topología resultante, cabe destacar que es un resumen de la misma, ya que la cantidad de nodos que se conectaron en la red eran demasiados. Luego dejamos aquellas con mayor cantidad de entradas y salidas dentro del grafo. El nodo sin dirección IP refiere a la agrupación de muchos otros nodos, para facilitar la visualización. Finalmente, en la topología se puede ver claramente, que en los paquetes del protocolo ARP, la dirección destino más frecuente era la **192.168.1.1**, que dada la red, podemos decir que es del router. Una dirección de un paquete ARP no esperada (o anómala) es la **0.0.0.0**. Esta dirección es la dirección que representa la dirección por defecto en las tablas de ruteo. Lo que nos hace suponer que la red tiene configurado una dirección por defecto para todos los paquetes que tienen como destino alguna red que no sea ninguna de las redes internas.

IV. Starbucks

Estas mediciones se realizaron un día Viernes por la tarde en un Starbucks frecuentado.

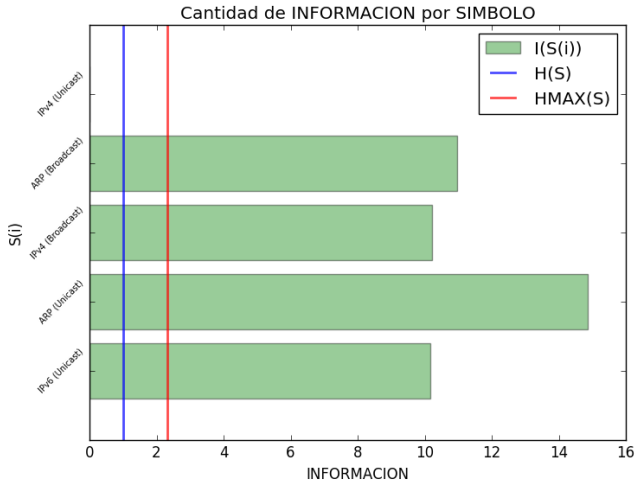
En principio, no tenemos información sobre la topología de la red, pero cabe mencionar que dicha conexión es abierta de Fibertel y para su uso es necesario el inicio de sesión.

IV.1. Fuente S_1

Para la fuente S_1 se obtuvieron los siguientes resultados:

Cuadro 7: *Starbucks, info. por símbolo*

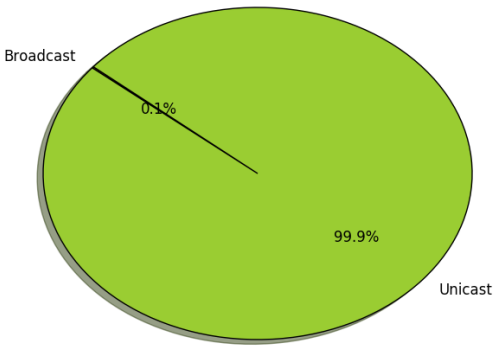
Datos fuente S_1		
TIPO	P(s_i)	I(s_i)
(Unicast, IPv4)	0.998	0.003
(Unicast, IPv6)	0.001	10.172
(Broadcast, IPv4)	0.001	10.229
(Broadcast, ARP)	0.001	10.966
(Unicast, ARP)	0.0	14.873
H(S_1) = 1 (0.03)		
$H_{max}(S_1)$ = 3 (2.32)		



Dado que estamos trabajando en una red abierta, de la cual no sabemos exactamente su topología, podríamos decir que la entropía de la misma se aleja de la máxima, dado que en una red abierta se pueden estar usando distintos protocolos (IPv4/IPv6 para enviar datos, ARP cuando un nuevo dispositivo se conecta, entre otras). La esperanza de que cada protocolo aparezca es pequeña.

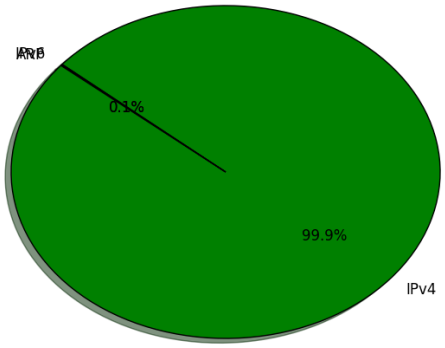
Luego, podemos ver que en nuestra tabla de resultados sucede lo previsto. La entropía es muy baja y distinta a la máxima que ocurre en ocaciones de equiprobabilidad.

A continuación podremos ver un gráfico que describe en porcentaje el destino del tráfico, tanto broadcast como unicast.



Esperábamos que al estar en una red abierta el tráfico broadcast sea mayor que el unicast, ya que los dispositivos se conectan y desconectan a la red con frecuencia. Esto no sucedió, suponemos puede deberse a que, aún bajo estas condiciones, no habían muchos dispositivos conectados por lo que entre ellos podían comunicarse. Cabe aclarar que la red no tenía una buena calidad de conexión y tiempos de sesión muy bajos.

Veamos más en detalle el porcentaje de los protocolos utilizados en esta red para sacar más concluciones:



Nuevamente, los protocolos hallados en esta red son los de IPv4, IPv6 y ARP de los cuales detallamos su función en una red con anterioridad.

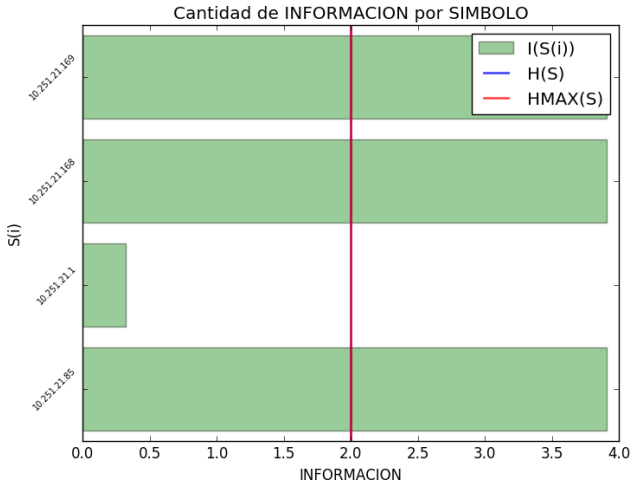
Por último, tomando como distinción nuevamente aquellos símbolos que están por debajo de la entropía podremos distinguir a $(Unicast, IPv4)$ que completaa nuestro estudio pudiendo ver que la mayoría de los dispositivos conectados son conocidos por la red y estan transmitiendo datos.

iv.2. Fuente S_2

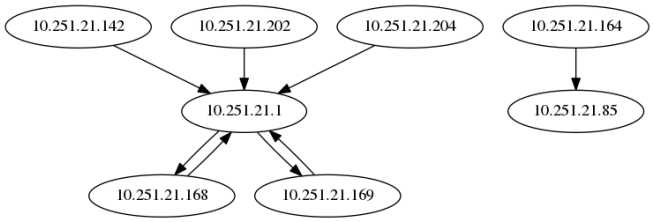
Para la fuente S_2 se obtuvieron los siguientes resultados:

Cuadro 8: *Starbucks, info. por símbolo*

Datos fuente S_2		
IP	P(s_i)	I(s_i)
10.251.21.1	0.8	0.322
10.251.21.169	0.067	3.907
10.251.21.168	0.067	3.907
10.251.21.85	0.067	3.907
H(S_2) = 2 (1.04)		
$H_{max}(S_2)$ = 2 (2.00)		



La primer particularidad que encontramos fue que la entropía redondeada era máxima. Se podría decir que no lo es, dado que $H(S_2) = 1.04$ y $H_{max}(S_2) = 2$, pero como la unidad se debe redondear, la entropía queda máxima. Dado la manera en que se configuraba la conexión a internet, lo unico que podemos saber es que hay un simbolo (el gateway) predominante, pero no encontramos motivos por el cual la entropia es máxima. Lo que sí dada la siguiente topología



Podemos encontrar que la IP **10.251.21.1**, por un lado es la única IP cuya información es menor a la entropía de la fuente, es decir tiene mayor cantidad de apariciones que el resto. Y por otro lado, en la topología es la IP destino en la mayoría de los paquetes ARP. Esto puede deberse, a que esa IP, es exactamente la del router.

Una anomalía encontrada, es una subred de dos nodos, el **10.251.21.164** y el **10.251.21.85**. Dado como esta configurada la red, no encontramos manera de justificarla. Además otra cuestión es que la IP **10.251.21.85** es parte de las direcciones destinos de los paquetes ARP.

V. Resultados globales y conclusiones

Durante el desarrollo de las consignas propuestas y el análisis de los datos obtenidos nos acercamos a las redes desde una mirada alternativa a la que usualmente se adopta. Desconociendo tamaños, topologías, configuraciones y dispostivos fuimos capaces de analizar la misma a través del tráfico de paquetes y sacar conclusiones basados en las herramientas provistas por la teoría de la información y los protocolos de las capas de link y de enlace del modelo OSI.

Luego de observar los distintos experimentos realizados sobre la fuentes **S1**, podemos concluir que existe una correlación positiva entre la entropía y la cantidad de hosts en una red. Notamos que al ordenar las redes utilizando como criterio la entropia de forma creciente obtenemos el mismo orden que al hacerlo por su jerarquía de tamaño.

Por otro lado, complementando el análisis desde la fuentes **S2**, podemos destacar que el **overhead** por tráfico ARP nunca superó el 30 % del total de los paquetes Ethernet intercambiados. Dicha proporción también está ligada al tamaño de la red, siendo aún mayor en las redes públicas donde hay mas conexiones esporádicas y de corta duración.

Complementando los resultados obtenido, a través de la fuente **S2**, logramos mostrar de manera exitosa la existencia de un nodo distinguido al que le corresponde la función de **default gateway**, respaldando la hipótesis que suponíamos. Es decir, esos eran para nosotros los nodos con menor información dada su alta participación en las redes a las que pertenecen. No logramos concluir, con el mismo análisis, ningún otro rol de los demas nodos activos en la red. En las redes públicas se suele dar el caso de nodos con actividad limitada en el tiempo, lo cual aumenta el grado de información de los mismos, pero no destaca ningún otro aspecto.

El análisis de los valores de entropía para las fuentes fue lo que nos permitió asociar al **default gateway** con los nodos que mostraban menor información con un grado de precisión que disminuye conforme lo hace el tamaño de la red. En la mayoría de los casos, los nodos cuya información es menor que la entropía, se corresponden con alguna funcionalidad particular dado que reciben un flujo mayor de tráfico de paquetes.

Por otra parte, cabe destacar que al crear fuentes de

información con las capturas, estamos recortando con cierto criterio nuestro campo de análisis. En el caso de S1, estamos centrándonos en símbolos representativos de los protocolos que viajan en la red, en cambio en S2 se destacan los nodos que participan de un solo protocolo dentro de todo ese intercambio de tramas. En el caso de dicho protocolo, la naturaleza de ARP, supone el envío y la recepción de paquetes con el fin de establecer la relación entre una **mac address** y una **ip address**, con lo cual podemos asegurar que los símbolos que componen S1 no son independientes entre sí e incluso existe cierto grado de proporcionalidad en la información (y también de su probabilidad respecto de los otros símbolos). En redes grandes es probable encontrar muchos paquetes de tipo broadcast, si es que los nodos permanecen poco tiempo conectados a la misma y requieren conexión al **default gateway**. Por otro lado, una vez que ese mapeo quedó realizado, la mayoría del consumo de ese tráfico tiene por destino **internet**, en consecuencia, la mayoría de esos paquetes de tipo ARP pasan a ser **unicast**.

La fuente S2, es un recorte distinto del tráfico que se analiza de cada red. En ese caso, estamos representando los nodos que son conectados mediante el protocolo ARP. Si bien hay independencia en la probabilidad entre los símbolos que componen la fuente, sabemos que el tráfico actual de una red tiene una preponderancia por el intercambio dirigido al exterior de la red (usualmente **internet**), con lo cual la probabilidad de encontrar al **default gateway** es mucho mas alta haciendo su información mucho mas baja que la del resto de los nodos.