DEPARTAMENTO DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

Trabajo Práctico

Wiretapping

Teoría de las Comunicaciones

Integrante	LU	Correo electrónico
Gonzalo Ariel Meyoyan	514/20	gonzalo@meyoyan.com
Alexandra Abbate	710/19	alexandra-abbate@hotmail.com
Cielo Serena Roccella	122/21	cielorocella@gmail.com
Florencia Rosenzuaig	118/21	f.rosenzuaig@gmail.com

Facultad de Ciencias Exactas y Naturales

Universidad de Buenos Aires

Ciudad Universitaria - (Pabellón I/Planta Baja)

Intendente Güiraldes 2160 - C1428EGA

Ciudad Autónoma de Buenos Aires - Rep. Argentina

Tel/Fax: (54 11) 4576-3359

http://www.fcen.uba.ar

1. Introducción

En este informe, presentamos un estudio realizado sobre las tramas capturadas en 4 redes distintas: una Fiesta, un host de Minecraft, un Centro Médico y una visualizacion de One Piece. Para el análisis, se utilizó la herramienta Wireshark, junto con una extensión del script provisto por la cátedra. Nuestro objetivo es identificar y resaltar patrones encontrados durante la examinación de los datos obtenidos, mostrando los resultados de manera intuitiva a través del uso de gráficos. A continuación, exhibiremos nuestros experimentos y conclusiones.

2. Métodos y condiciones de los experimentos

2.1. Nuestro programa

Para realizar la experimentación, usamos Wireshark para sniffear las tramas de la red. Luego, implementamos un código que por cada trama obtenida, forma una tupla $s_i = \langle$ *tipo del destino, protocolo de la capa superior inmediata* $\rangle$. Modelamos la fuente de información nula $S1$ como el conjunto de todas las tramas obtenidas, es decir, $S1 = \{s_1, s_2, s_3, ..., s_n\}$. Finalmente, una vez que tuvimos $S1$ armado, por cada s_i nos fijamos su tipo de destino, su protocolo de capa superior inmediata y su cantidad de apariciones para calcular la entropia total, la cantidad de información de cada s_i, el porcentaje Broadcast/Unicast y el porcentaje de aparición de cada protocolo encontrado.

2.2. Extensión de nuestro programa

Para encontrar nodos distinguidos, construimos el conjunto $S2$. Por cada trama ARP obtenida, formamos el símbolo $s'_i = \langle$ dirección IP src $\rangle$. Luego, $S2 = \{s'_1, s'_2, s'_3, ..., s'_m\}$.

El protocolo ARP permite a partir de una dirección IP conseguir la dirección MAC. El router es quien se encarga de mantener la tabla de ARP, por lo que va a ir preguntando por la red las direcciones MAC de cada host (mandando paquetes ARP) para mantener la tabla correcta. Por esto, decidimos que los símbolos de $S2$ se distingan por su dirección IP src, porque sospechamos que el nodo distinguido va a ser el router.

2.3. Redes analizadas

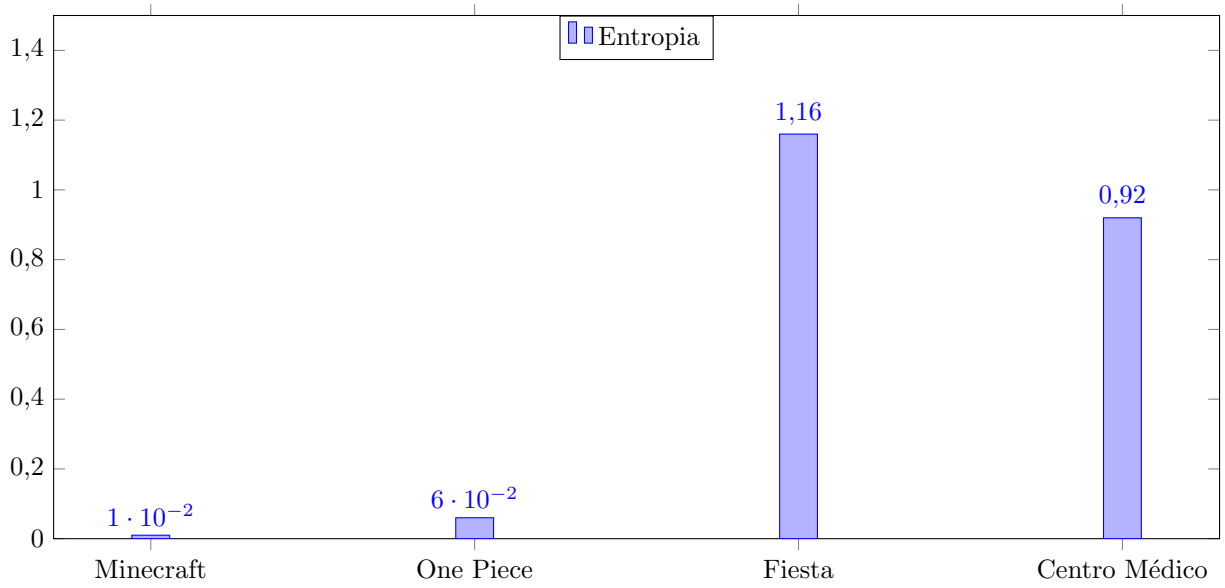
Corrimos nuestro programa en 4 redes distintas:

- **Minecraft:** Red WiFi de la casa de Gonzalo Meyoyan, durante el hosting de un servidor de Minecraft involucrando el acceso de personas por fuera de la red local. La captura fue realizada el 18 de septiembre a las 22:46, con una duración de aproximadamente 15 minutos. En total, se capturaron 1.407.942 paquetes.
- **One Piece:** Red WiFi de la casa de Florencia Rosenzuaig mientras alguien veia una serie[*]. La captura fue el 22 de septiembre a las 23:05hs. Se capturaron 22119 paquetes en 5 minutos. Había 4 personas conectadas.
- **Fiesta:** Red WiFi de la casa de Florencia Rosenzuaig durante un cumpleaños. La captura fue el domingo 17 de septiembre desde la 1:40 AM hasta las 1:50 AM. Se capturaron 16926 paquetes en un lapso de 10 minutos. Había un estimado de entre 15 a 25 personas conectadas a la red.
- **Centro Médico:** Red WiFi del centro médico Mevaterapia durante horario laboral. La captura fue el lunes 18 de septiembre desde las 15:47 PM hasta las 15:53 PM. Se capturaron 50000 paquetes en un lapso de 5 minutos.

[*] https://aniwave.to/watch/one-piece.ov8/ep-1

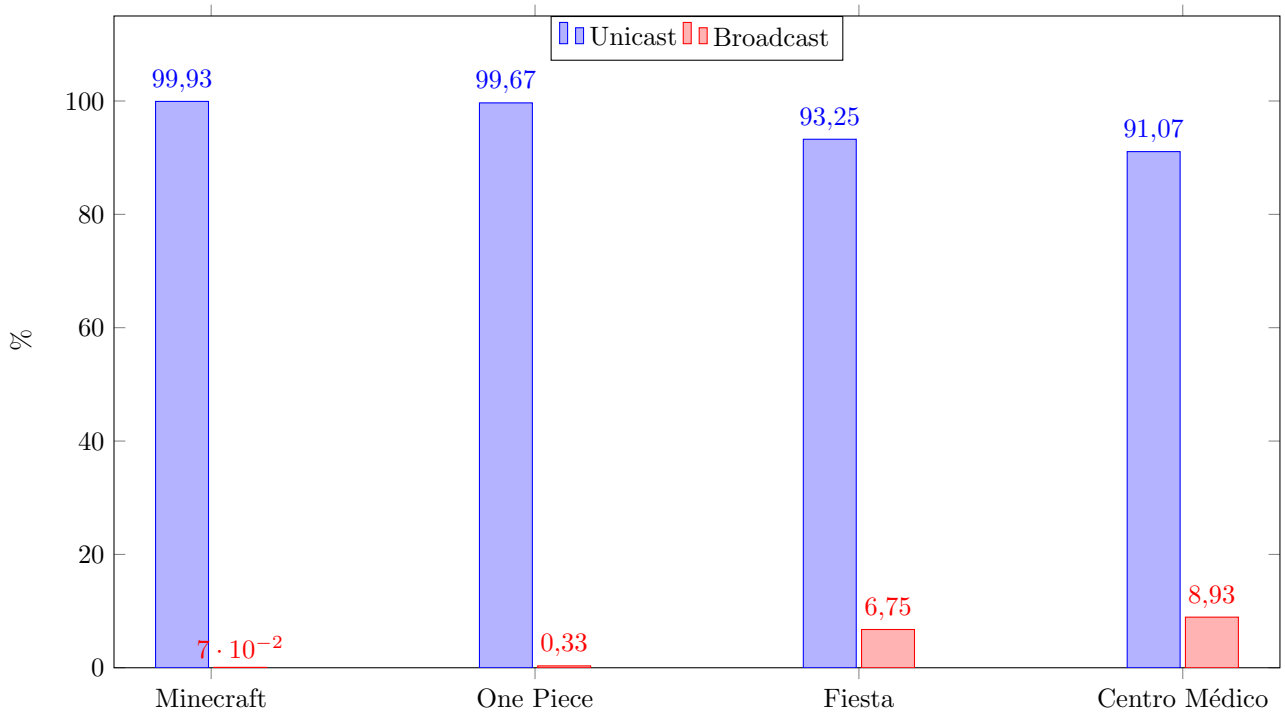
3. Análisis de la fuente $S1$

3.1. Entropía de cada red analizada



La entropía mide la heterogeneidad de una red. Puede observarse que las redes One Piece y Minecraft tienen menor entropía que en las redes Fiesta y Centro Médico. Es muy razonable que las dos primeras tengan menor heterogeneidad, dado que éstas son redes con muy pocos usuarixs y que están realizando una única tarea principal (mostrar la serie o sostener el servidor). A su vez, es lógico que las redes de la Fiesta y del Centro Médico tengan mayor entropía, ya que se encontraban varios dispositivos distintos conectados realizando tareas distintas.

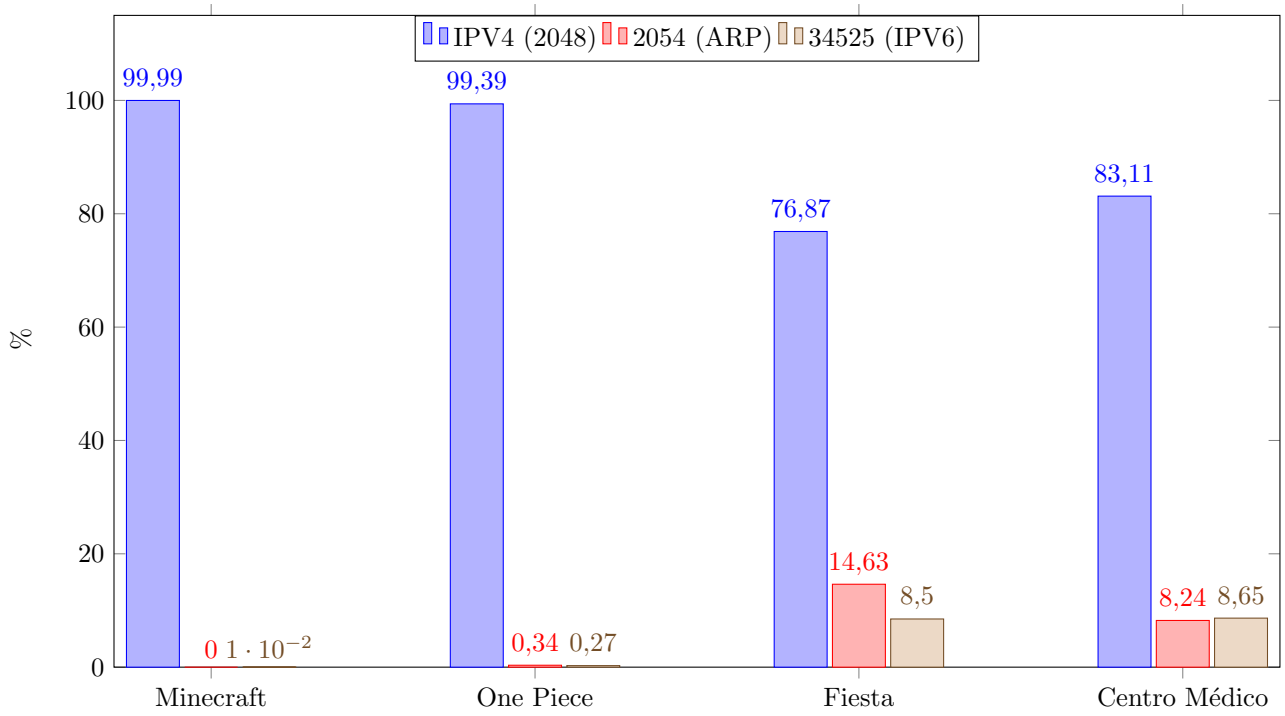
3.2. Porcentaje de tráfico Broadcast/Unicast sobre el tráfico total



Este gráfico presenta el porcentaje de trafico Broadcast y Unicast en las redes analizadas. Los paquetes Unicast se envían de punta a punta, mientras que los paquetes Broadcast se envían a todos los dispositivos de la red. Podemos observar como el trafico Unicast es mucho más prevalente que su contraparte, lo cual parece respaldar el hecho de que los recursos de la red se utilizan principalmente

para la comunicación punto a punto.

3.3. Porcentaje de aparición de cada protocolo encontrado

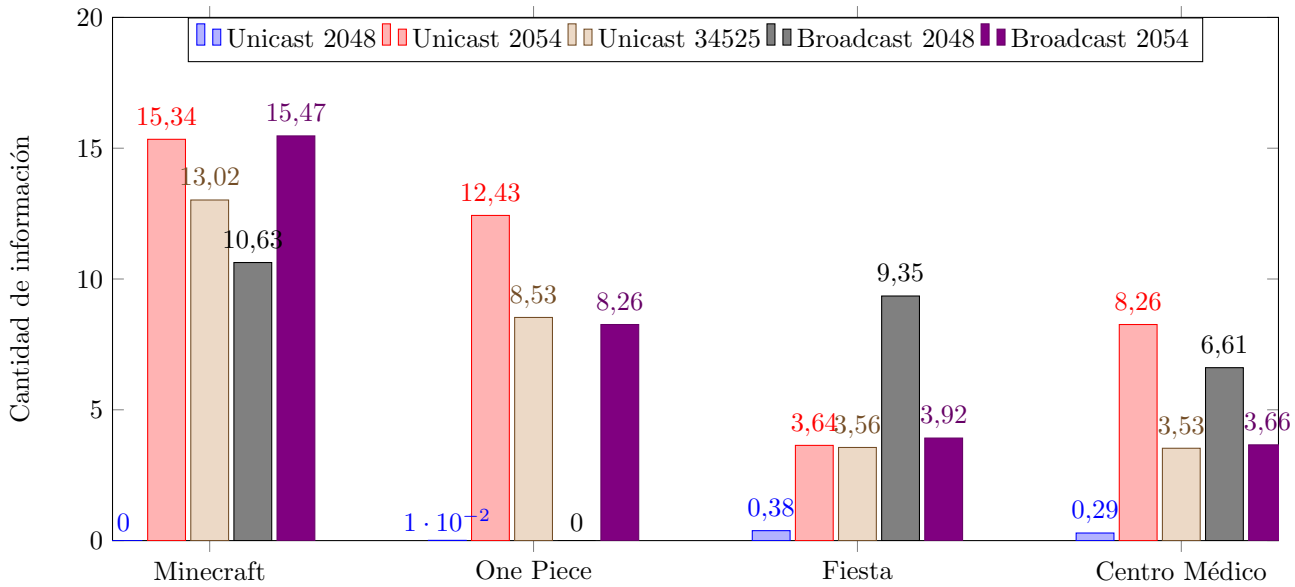


En el gráfico se evidencia como para la red Minecraft casi todos los paquetes se corresponden al protocolo IPv4, tiene sentido que la mayoría de paquetes correspondan al envío de datos cuando la red esta manteniendo el servidor del juego activo, Son tantos los paquetes de datos que se envían que los paquetes del protocolo ARP pasan a ser un porcentaje muy pequeño del total de datos enviados. Caso parecido aunque no tan extremo pasa con la red One Piece, la mayoría de los paquetes son IPv4, asumimos que son los datos para ver la serie.

En el caso de la fiesta y el centro médico se pueden observar muchos más paquetes correspondientes al protocolo ARP, tiene sentido ya que en estas redes no se estaba haciendo una transferencia grande de datos, además de que con muchos dispositivos conectados se hacen más controles para mapear IP con MAC.

También notamos que hay muchos mas paquetes IPv4 que IPv6, un resultado esperado siendo que IPv4 es mucho más utilizado que IPv6.

3.4. Cantidad de información de cada símbolo



En este gráfico se evidencia como la cantidad de información de los símbolos es inversamente proporcional a la cantidad de ocurrencias de los mismos. Notamos que en todos los casos Unicast para el protocolo IPv4 es el símbolo que más se envió, con lo cuál es claramente el símbolo con menos información.

En particular en el caso de la red del servidor de Minecraft todos los símbolos que no aparecieron tanto como Unicast IPv4 tienen una cantidad de información alta, estos son los que menos tienen incidencia en el calculo de la entropía, por muy altos que sean la entropía es baja ya que estos no la afectan mucho.

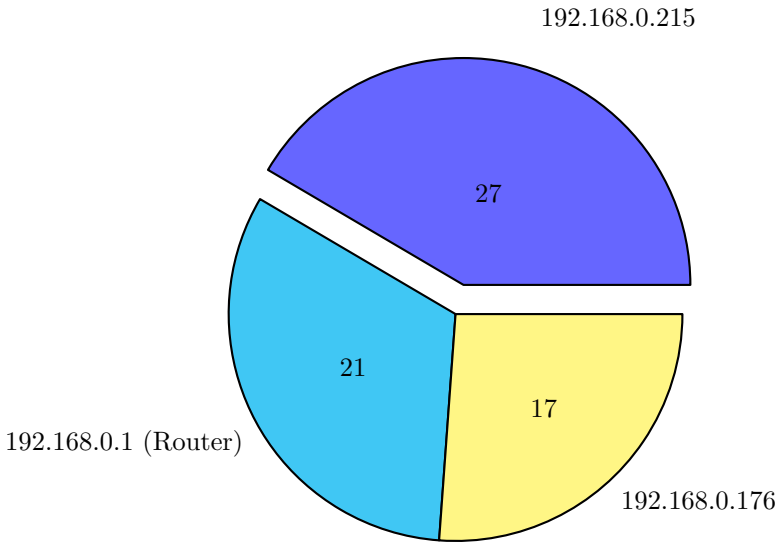
La red que tenía mayor entropía, la de la fiesta, es la red en la que la cantidad de información brindada por los símbolos es más uniforme, esto es razonable ya que se corresponde con la definición de entropía.

4. Análisis de la fuente $S2$ (Opcional)

A continuación vamos a explicar la segunda parte del experimentación. De ahora en más vamos a analizar exclusivamente los paquetes ARP de las mismas redes, introducimos una nueva fuente de información nula llamada $S2$.
Con el objetivo de encontrar nodos distinguidos, por cada red vamos a ver cuáles son las IPs que más paquetes ARP recibieron.

4.1. Red Minecraft

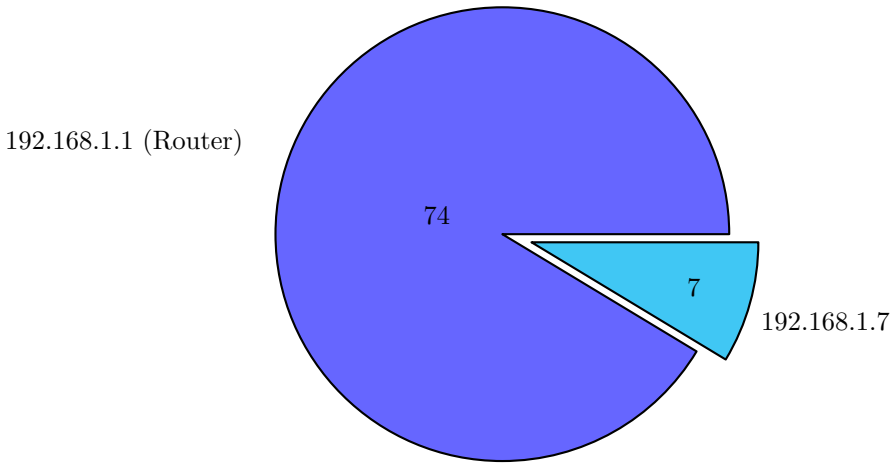
Todas las IPs que enviaron paquetes ARP:



Nos llamó la atención que la IP que más paquetes ARP recibió no era el router. Entonces, nos metimos en la configuración del router y encontramos que curiosmanete el dispositivo que más paquetes ARP recibió es uno de los celulares conectados a la red. No estamos seguros de cuál es la razón por la que ésto sucedió.

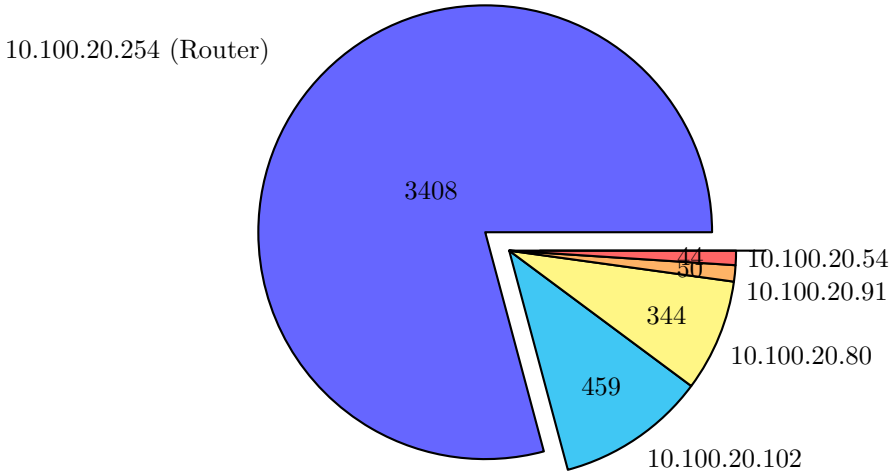
4.2. Red One Piece

Todas las IPs que enviaron paquetes ARP:



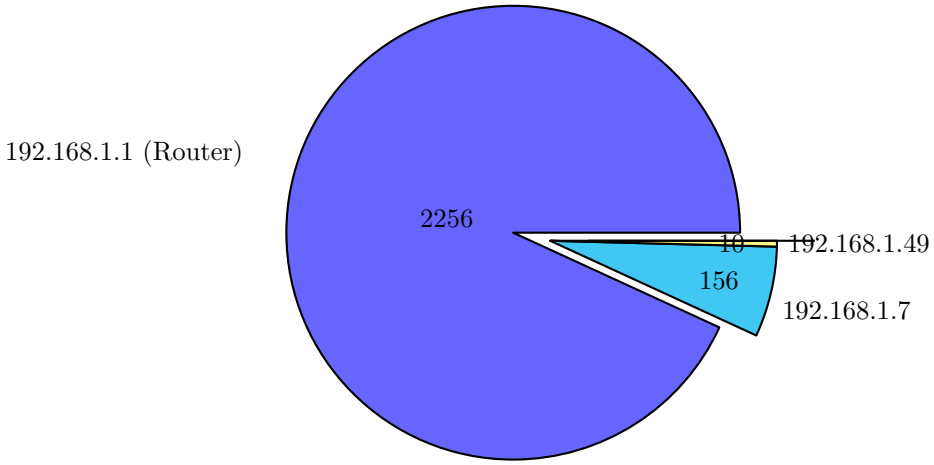
4.3. Red Centro Médico

Las 5 IPs que más enviaron paquetes ARP:

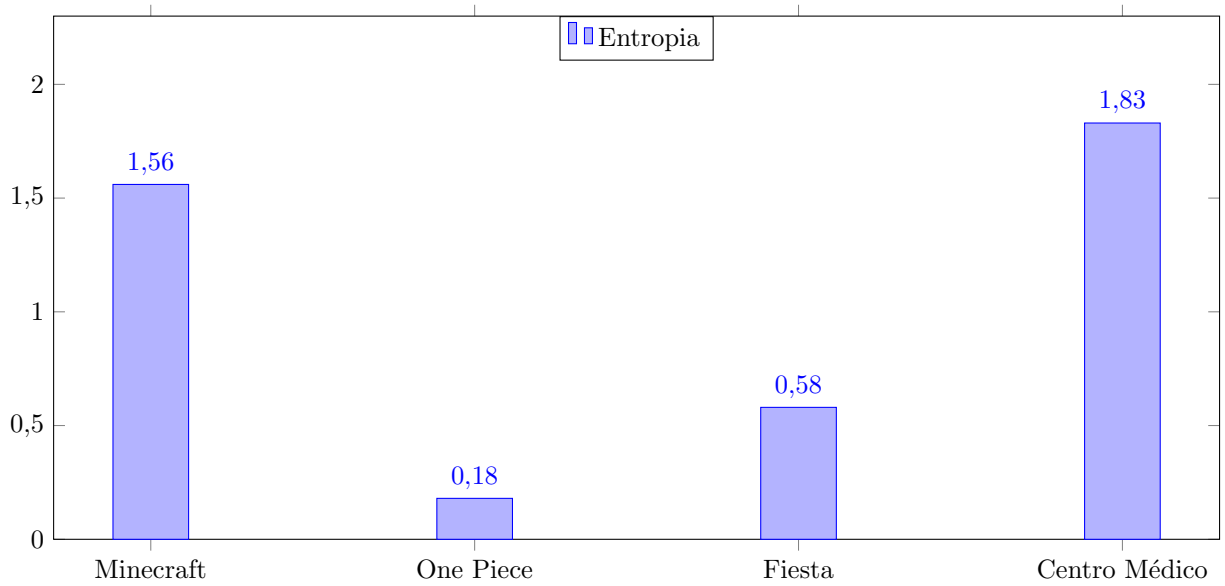


4.4. Red Fiesta

Las 3 IPs que más enviaron paquetes ARP:



4.5. Entropía de la fuente $S2$ para cada red

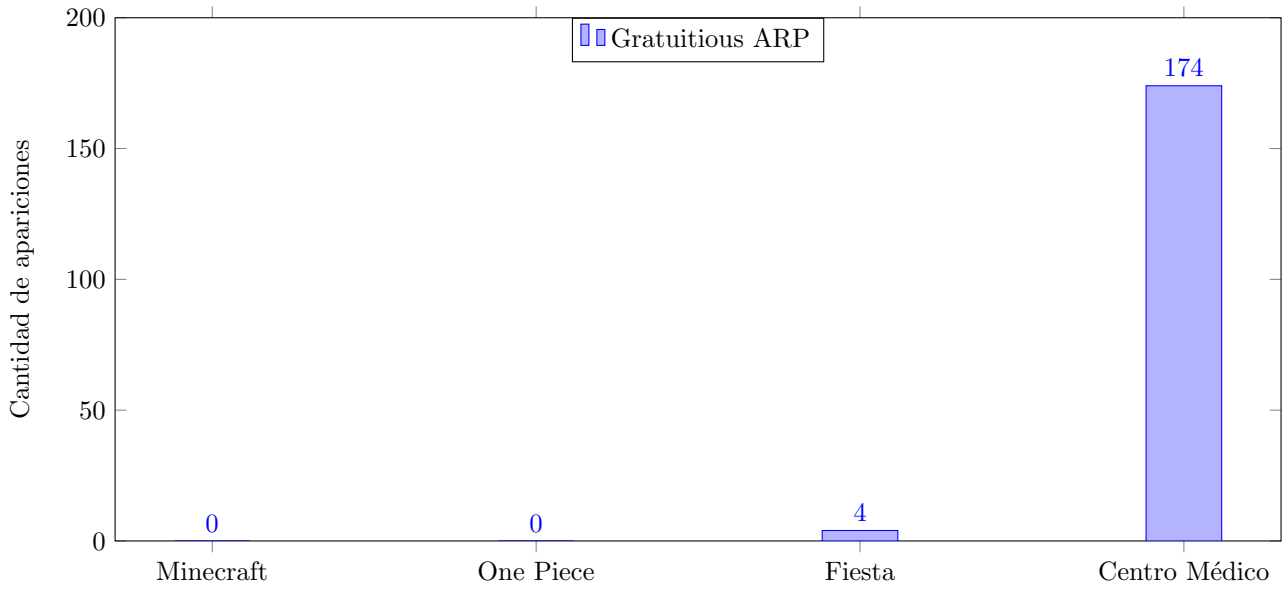


La entropía representa la variación en cantidad de información de cada dirección IP que envía paquetes ARP. Mayor entropía (por ejemplo, Centro Médico) indica que en la red hay mucha disparidad en la cantidad de paquetes ARP que envía cada IP.

4.6. Apariciones de paquetes ARP inesperados

Analizando las capturas con Wireshark, encontramos que en ciertas redes hay Gratuitious ARP. Estos son envíos de anuncios de una dirección IP y MAC en una red que no fueron solicitados previamente. Su principal uso es informar a todos los demás dispositivos de un cambio en la red. Estos son algunos casos de uso:

- Un dispositivo modifica su MAC address manualmente. El dispositivo en cuestión podria entonces enviar un Gratuitious ARP para actualizar el mapeo ARP del resto de dispositivos en la red.
- Cuando un nuevo dispositivo se conecta a la red, este paquete ser enviado para anunciar su existencia.
- Hay redundancia en la red: Situaciones en las que dispositivos que comparten IP y/o MAC son usados de manera redundante para proveer tolerancia a fallos. En este caso, el envío de Gratuitious ARP es permite garantizar la capacidad de comunicarse continuamente con la IP en cuestión, mientras cambia entre los dispositivos.



5. Conclusiones

A partir de las capturas obtenidas, llegamos a ciertas conclusiones. En primer lugar, la entropía de cada red refleja con claridad la cantidad de actividad de las mismas. Aquellas redes con mayor actividad presentan mayor entropía y viceversa. Observamos que ninguna red alcanzó su entropía máxima teórica, ya que para ello todos sus símbolos deberían ser iguales. Por otro lado, nos dimos cuenta que la cantidad de tráfico Unicast es significativamente mayor que el de tráfico Broadcast. Ésto significa que la mayoria de las comunicaciones se realizan punto a punto. Sin embargo, hay que tener en cuenta que la muestra puede no ser representativas del comportamiento general de la red. Por ejemplo, Florencia no suele hacer fiestas grandes y Gonzalo no suele mantener un servidor de Minecraft.

Encontramos tres protocolos distintos: IPV4 (2048), IPV6 (34525) y ARP (2054). IVP4 e IPV6 transportan datos y ARP es un protocolo de control. IPV4/6 son el protocolo IP y se encargan del envio de paquetes. IPV4 tiene direccionamiento de 32 bits e IPV6 de 128. Por otro lado, ARP sirve para hacer la conversión entre MAC address e IP.

5.1. Conclusiones (Opcional)

Respecto a la entropía, en ninguna de las redes analizadas se alcanza la entropía máxima teórica, pues no se da la condición de que los símbolos de la fuente sean equiprobables. Esto sugiere que existe cierta predecibilidad en el trafico de la red, con algunos dispositivos siendo mas propensos al envío de paquetes ARP que otros. Este comportamiento se alinea con nuestras expectativas, pues se espera que haya dispositivos como el router que envíen mas de estos paquetes, en comparación al resto de miembros en la red.

Además, en cada red observamos que la cantidad de envíos de paquetes ARP por IP resulta ser un indicador confiable que nos permite distinguir al router de la misma. En todas las redes excepto Minecraft, el dispositivo asociado a la IP con mas envíos ARP resulta ser el router, mientras que en la red Minecraft, resulta ser el segundo con mas envíos.

Finalmente, deducimos que la marcada disparidad entre la red del Centro Médico y el resto de redes locales en cuanto a paquetes Gratuitious ARP se debe principalmente a la gran cantidad de dispositivos conectados y la frecuencia con la que se conectan y desconectan dispositivos a la red.