DEPARTAMENTO
DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Trabajo Práctico 1 - Wiretapping

Martes 23 de Septiembre — Teoría de las Comunicaciones

Integrante	LU	Correo electrónico
Santiago Aboy Solanes	175/12	santiaboy2@hotmail.com
Emilio Almansi	674/12	ealmansi@gmail.com
Federico Canay	250/12	fcanay@hotmail.com
Facundo Decroix	842/11	fndecroix92@hotmail.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

Índice

1. Introducción

En este trabajo práctico vamos a abordar el desarrollo de herramientas de diagnóstico de red. Nuestro objetivo va a ser analizar estadísticamente el protocolo ARP. Por otro lado, vamos a sacar conclusiones acerca de los tipos de dispositivos de red que se pueden encontrar en un segumento de red determinado. Para ello, utilizamos la herramienta de manipulación y análisis de paquetes, Scapy.

2. Desarrollo

Antes de comenzar el desarrollo vamos a definir algunos términos.

• **Informacion**: Dado un evento E decimos que cuando E tiene lugar, recibimos

$$I(E) = log(\frac{1}{P(E)})$$

unidades de información. Al usar log_2 la unidad obtenida es bits.

• **Entropía**: La entropía de un mensaje X, que se representa por H(X), es el valor medio ponderado de la cantidad de información de los diversos estados del mensaje

$$H(X) = -\Sigma\ p(x)\ log\ p(x)$$

• **Nodo distinguido**: En una fuente, un nodo distinguido es un nodo cuya información es menor a la entropía de dicha fuente.

2.1. Capturando tráfico

Para el desarrollo de este trabajo práctico escuchamos pasivamente redes para poder observar que sucedía en las mismas. En particular, capturamos paquetes ARP *who-has*.

Utilizamos dos modelos de fuente de información:

$S_{dst} = \{s_1 \cdots s_n\}$ siendo s_i una IP que aparece como dirección destino en los paquetes ARP *who-has*

$S_{src} = \{s_1 \cdots s_n\}$ siendo s_i una IP que aparece como dirección origen en los paquetes ARP *who-has*

Creamos una *tool* que escucha pasivamente en la red local. Luego, la adaptamos para que estime las probabilidades de dichas fuentes en función de los paquetes ARP observados y que calcule la entropía de las mismas.

Usando dicha herramienta, realizamos capturas de paquetes ARP sobre distintas LANs: Alto Palermo, Red laboral de Honeywell, Laboratorios de Ciudad Universitaria (Via Wi-Fi), y la casa de un integrante del grupo.

2.2. Gráficos y análisis

Una vez que capturamos el tráfico, nos propusimos gráficar y a analizar los datos obtenidos. Graficamos en forma de histogramas, y de grafos la información y entropía de S_{dst} y S_{src}

3. Resultados

3.1. Red Alto Palermo

3.1.1. Descripción y topología de la red

lugar, dia de la semana, hora aproximada, fecha, wifi o ethernet cantidad de paquetes tomados, tiempo de muestreo

Nuestro primer experimento consistió en medir la LAN Wi-Fi pública del shopping Alto Palermo. Esta medición se llevó a cabo el Sábado 20 de Septiembre a las 21hs, el tiempo de medición fue de aproximádamente 40 minutos y se capturaron 1569 paquetes ARP.

Figura 1: Grafo Medición Alto Palermo

3.1.2. Topología de la red

A continuación mostramos un grafo que muestra los nodos de la red con su dirección IP y la cantidad de mensajes de tipo *who-has*.

Como podemos ver en el grafo, la red tiene un nodo distinguido. Este nodo, el cual tiene la dirección IP 117.17.12.1, recibe muchos mensajes de la mayoría de los otros nodos de la red, pero no envía ninguno. Suponemos que este nodo es el router de la red.

3.1.3. Fuente: S_{dst}

A contincuación mostramos los gráficos

3.1.4. Fuente: S_{src}

histograma grafico de informacion entropía total

3.1.5. Discusión

cualquier cosa interesante sobre este caso en particular

3.2. Red Honeywell

3.2.1. Descripción y topología de la red

lugar, dia de la semana, hora aproximada, fecha, wifi o ethernet cantidad de paquetes tomados, tiempo de muestreo

Nuestro segundo experimento consistió en capturar los paquetes de la LAN Wi-Fi de la empresa Honeywell. En esta red no hay mucho tráfico, ya que la mayoría de las computadores se conectan via Ethernet a una VPN. Esta red es dedicada a transacciones que no necesiten un nivel de seguridad. La captura se realizo un día lunes a las 11 am. durante media hora, lográndose capturar 253 paquetes.

3.2.2. Topología de la red

grafico del grafo de la red

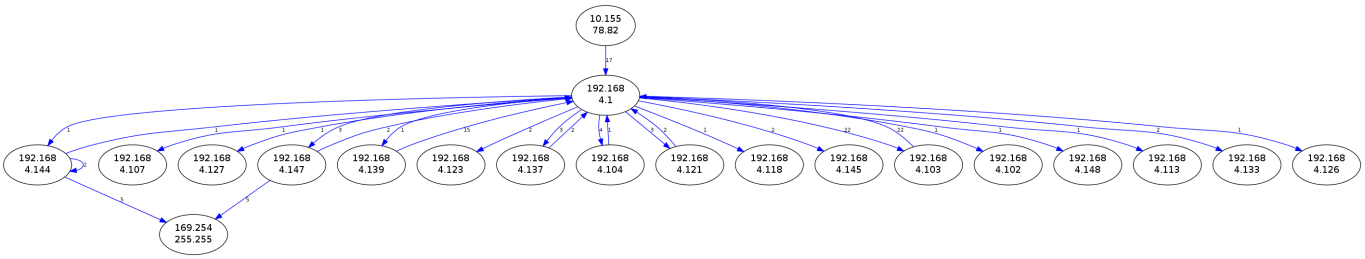

Figura 2: Medición Honeywell

3.2.3. Fuente: S_{dst}

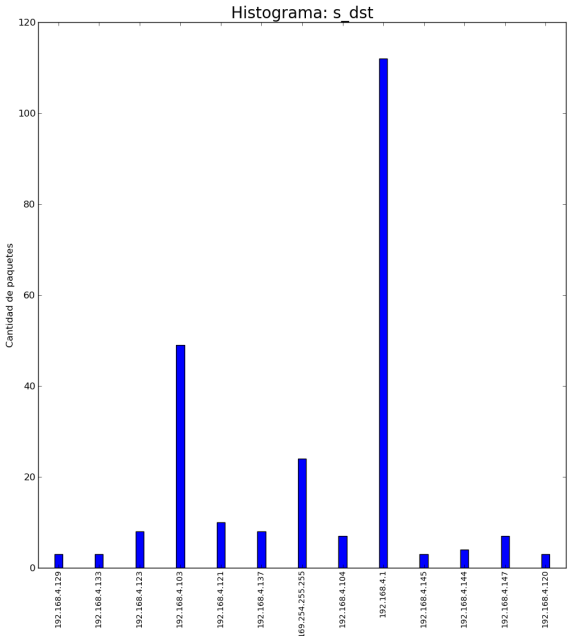

Figura 3: Medición Honeywell

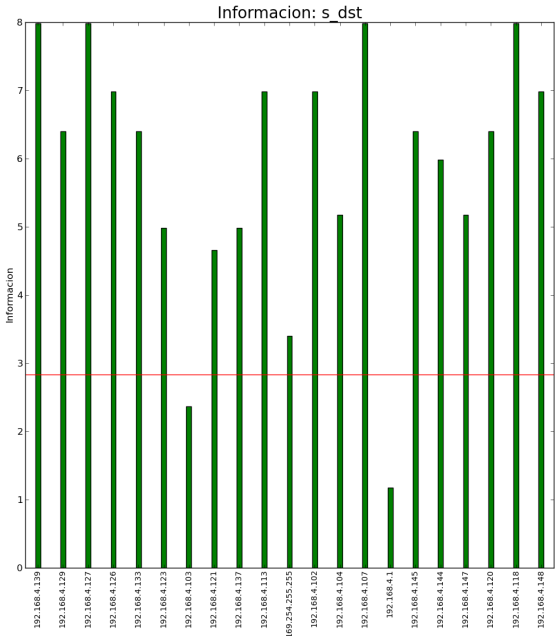

Figura 4: Medición Honeywell

histograma grafico de informacion entropía total

3.2.4. Fuente: S_{src}

histograma grafico de informacion entropía total

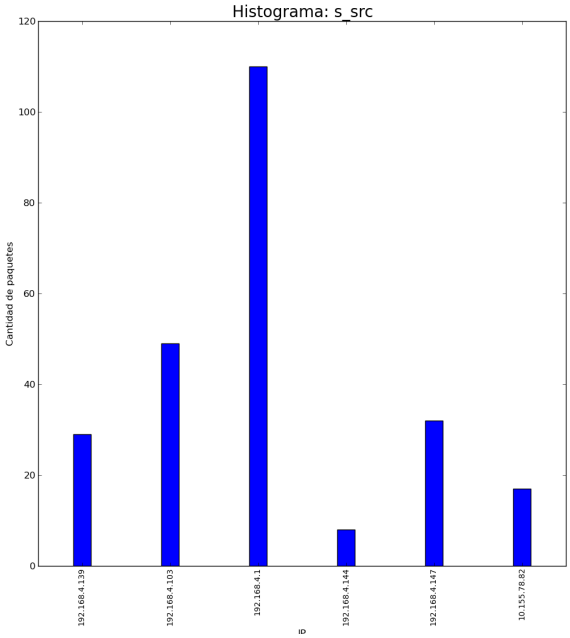

Figura 5: Medición Honeywell

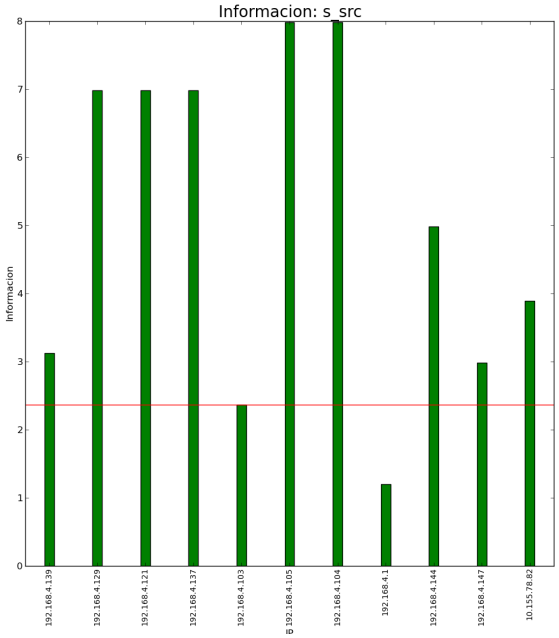

Figura 6: Medición Honeywell

3.3. Red Laboratorios DC

3.3.1. Descripción y topología de la red

Realizamos una captura en la red Wi-Fi *Entrepiso-DC*, disponible desde los laboratorios del Depto. de Computación. La muestra fue tomada un lunes a las 17hs aproximadamente -horario típicamente de alto tráfico-, logrando un total de XX paquetes en MM minutos.

En el gráfico de la figura 7 se presenta el grafo dirigido representando la red. En el mismo se observa una gran cantidad de nodos ligada al nodo con IP 10.1.200.197, y luego múltiples conjuntos pequeños de nodos conectados entre sí pero disconexos de la estructura mayoritaria.

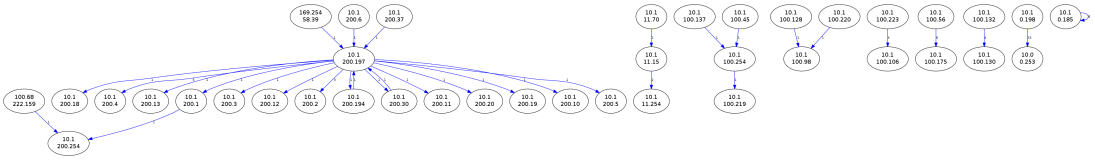

Figura 7: Grafo mostrando la topología de la red *Entrepiso-DC*.

3.3.2. Fuente: S_{dst}

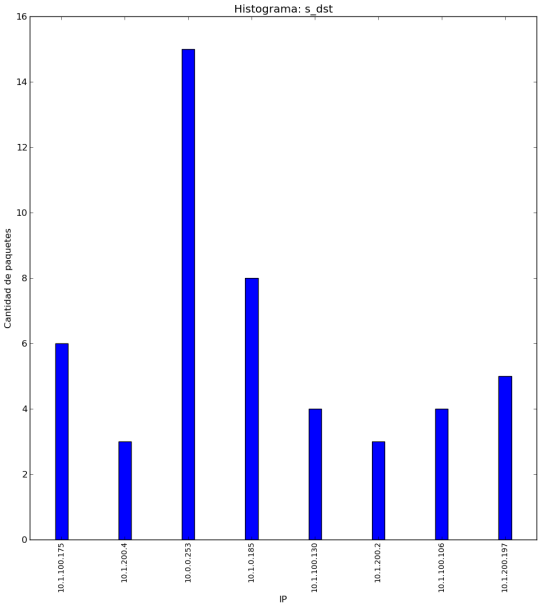

Figura 8: Histograma de la serie de paquetes s_dst de la red *Entrepiso-DC*.

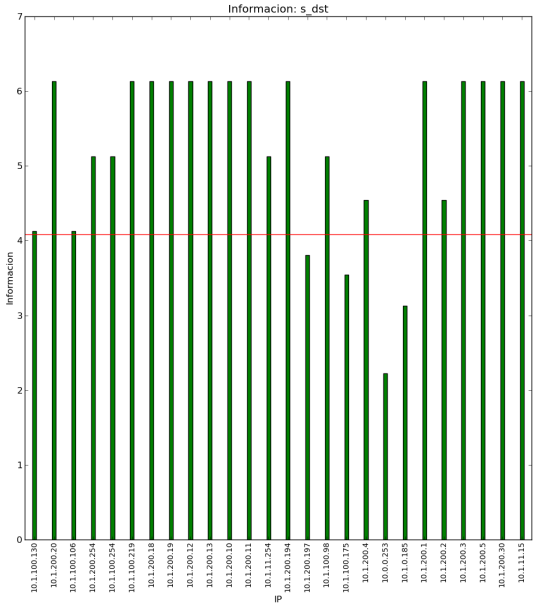

Figura 9: Gráfico de cantidad de información para cada IP s_dst de la red *Entrepiso-DC*.

entropía total

3.3.3. Fuente: S_{src}

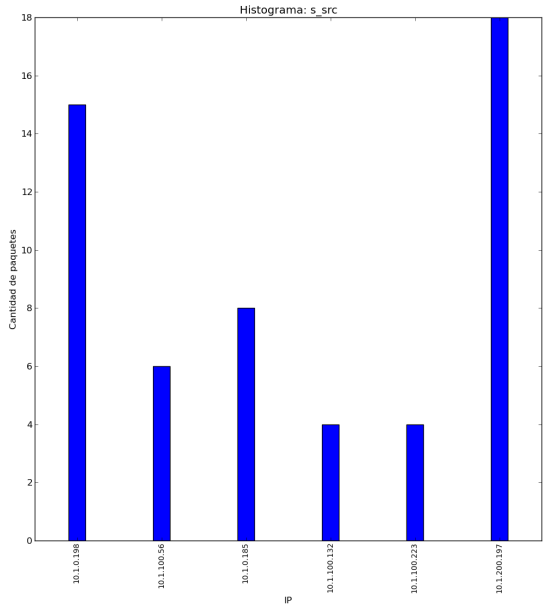

Figura 10: Histograma de la serie de paquetes s_src de la red *Entrepiso-DC*.

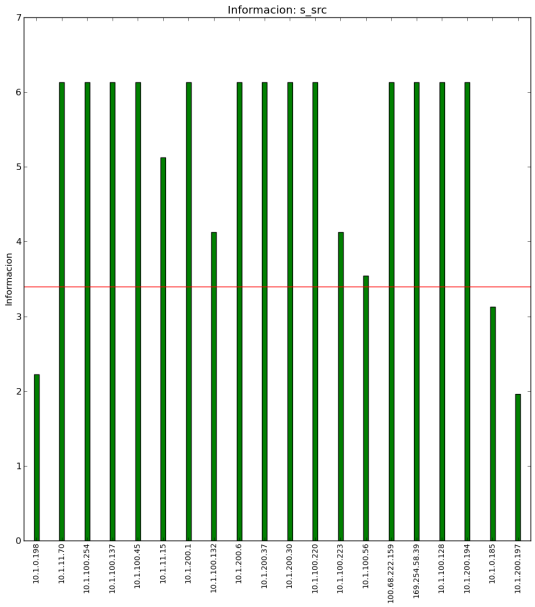

Figura 11: Gráfico de cantidad de información para cada IP s_src de la red *Entrepiso-DC*.

entropía total

3.3.4. Discusión

cualquier cosa interesante sobre este caso en particular

3.4. Red hogareña

3.4.1. Descripción

Para nuestro último experimento, capturamos el tráfico de la LAN de un integrante de nuestro grupo. Medimos el Miércoles 17 de Septiembre a las 00:00 utilizando la red Wi-Fi. El tiempo de medición fue de aproximadamente 40 minutos, y capturamos aproximadamente 20 paquetes.

3.4.2. Topología de la red

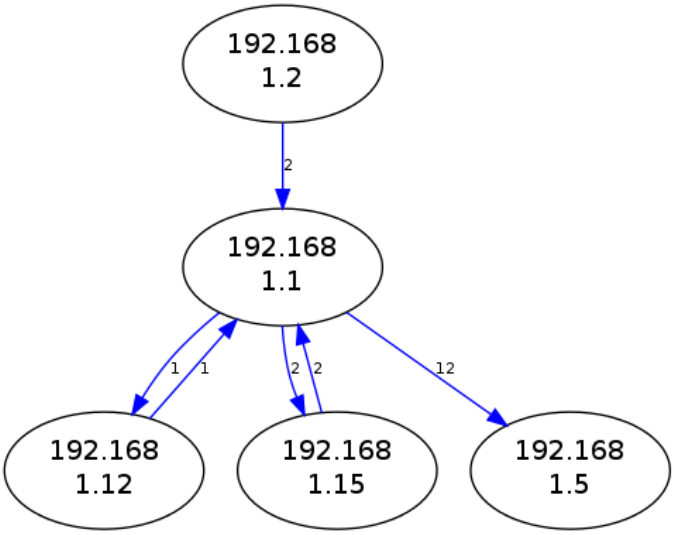

Figura 12: Grafo de LAN hogareña

3.4.3. Fuente: S_{dst}

- Entropía de la fuente: 1.49046857073

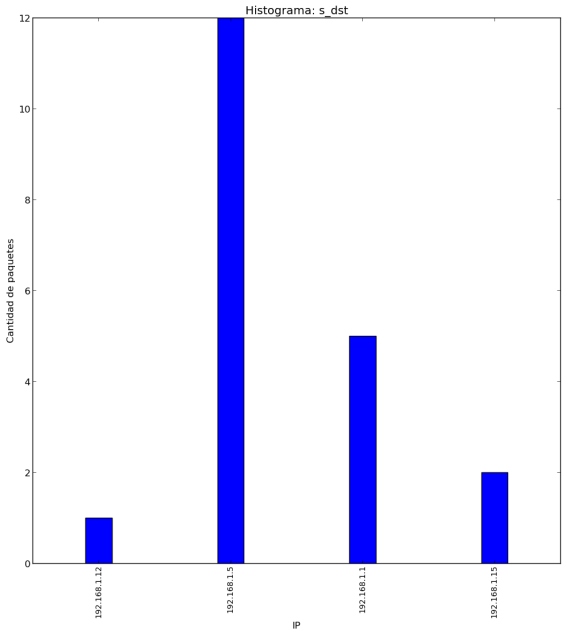

Figura 13: Histograma de S_{dst}

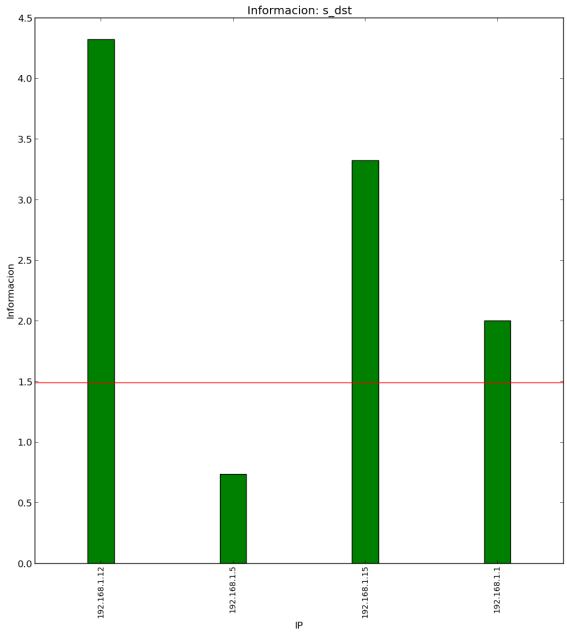

Figura 14: Informacion de S_{dst}

3.4.4. Fuente: S_{src}

- Entropía de la fuente: 1.19176014818

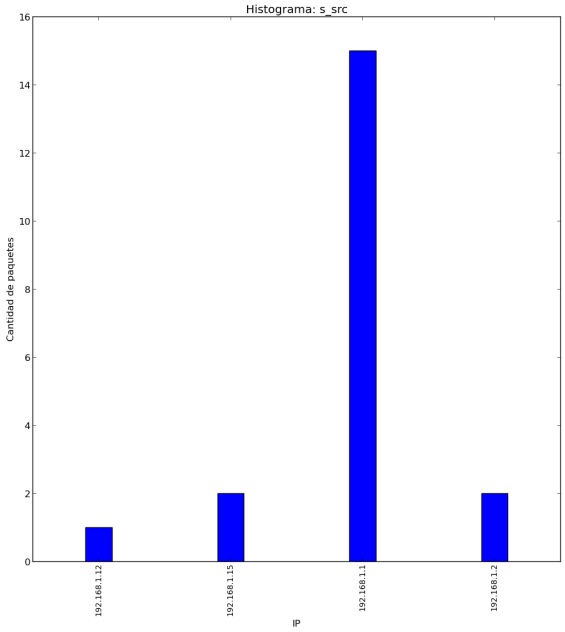

Figura 15: Histograma de S_{src}

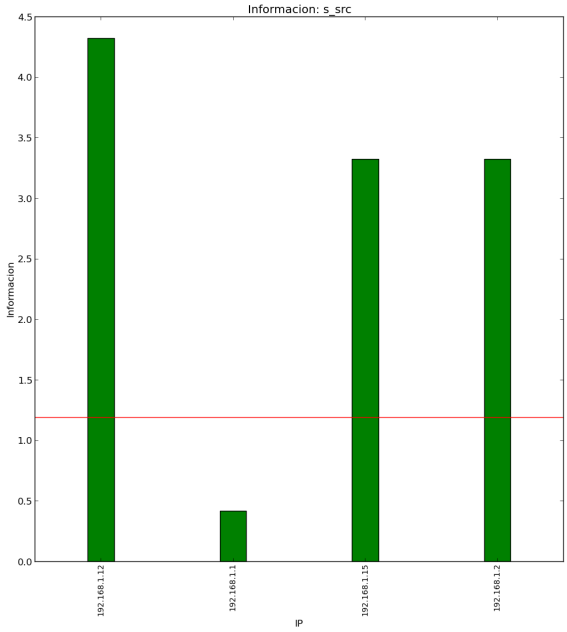

Figura 16: Informacion de S_{src}

3.4.5. Discusión

cualquier cosa interesante sobre este caso en particular

4. Discusión general

5. Conclusión

Como conclusión, queremos recalcar que por lo general los routers son nodos distinguidos en las LANs a las que pertenecen. Esto se mantiene, ya sea una red pública o privada.

Como pudimos ver en los experimentos, creemos que es importante saber que esto no necesariamente siempre es así. En el caso de Ciudad Universitaria, el servidor local era un nodo distinguido.

Para finalizar, en este trabajo práctico aprendimos que LA AMISTAD RESUELVE TODOS LOS PROBLEMAS.