Teoría de las Comunicaciones

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

Trabajo Práctico 1A: *Wiretapping*

Integrante	LU	Correo electrónico
Antonio, Pablo	290/08	pabloa@gmail.com
Ferrari, Gastón	775/07	gastonferrari5@hotmail.com

1. Introducción

El presente informe corresponde al Trabajo Práctico 1A, titulado "*Wiretapping*", de la materia Teoría de las Comunicaciones. El objetivo de este trabajo es desarrollar una herramienta sencilla de diagnóstico de red y realizar un análisis a partir de la información que esta nos provee en distintos segmentos de red.

2. Análisis de entropía

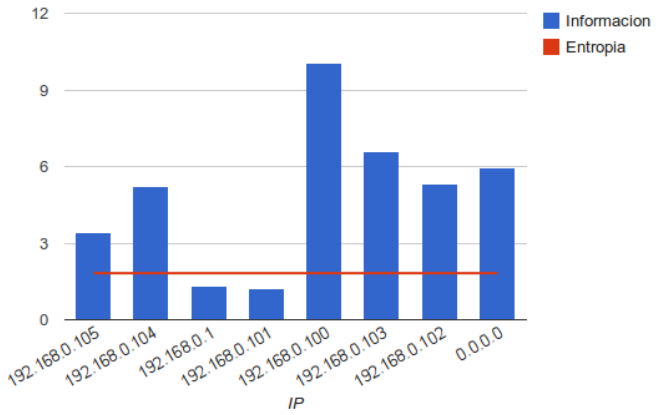
Para este punto decidimos tomar como símbolos de la fuente de información a las direcciones IP de los nodos de una red de hogar. Como modelo vamos a analizar los datos de diferentes maneras:

2.0.1. Primera red (6 horas de capturas de paquetes):

- IPs que realizaron consultas ARP:

Símbolo	Consultas	Probabilidad	Información
192.168.0.105	99	0.0947368421053	3.39993060689
192.168.0.104	28	0.0267942583732	5.22193230491
192.168.0.1	448	0.428708133971	1.22193230491
192.168.0.101	415	0.397129186603	1.33231970073
192.168.0.100	1	0.000956937799043	10.029287227
192.168.0.103	11.0	0.0105263157895	6.56985560833
192.168.0.102	26	0.0248803827751	5.32884750883
0.0.0.0	17	0.0162679425837	5.94182438572

Entropía de la fuente:
$H(S) = 1{,}82297065237$



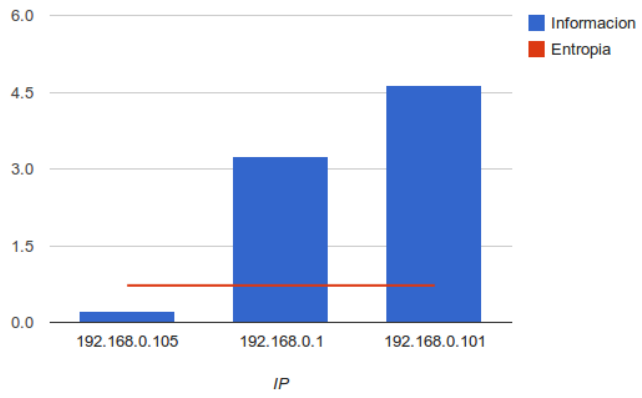
En este caso la IP que realizó más consultas ARP fue 192.168.0.1 (router), ésto es lógico considerando que el router es el encargado de distribuir todo el tráfico de la red a los nodos correspondientes por lo que su tabla de direcciones macs tiene que estar correctamente actualizada el mayor tiempo

posible.

- IPs que respondieron consultas ARP:

Símbolo	Respuestas	Probabilidad	Información
192.168.0.105	506	0.85472972973	0.226459790935
192.168.0.101	24	0.0405405405405	4.62449086491
192.168.0.1	62	0.10472972973	3.25525705524

Entropía de la fuente
$H(S) = 0{,}721963466885$

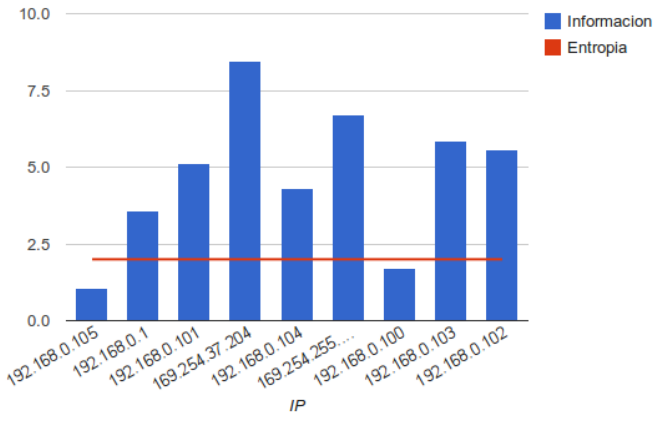


En este caso la IP 192.168.0.105 fue la que más veces contestó los pedidos sobre su MAC, aumentando su probabilidad. Como se puede observar, la información aportada por esta IP es considerablemente más baja que la aportada por las demás que poseen menor probabilidad e incluso más baja que la entropía de la red.

- IPs por las que se realizaron consultas ARP:

Símbolo	Consultas	Probabilidad	Información
169.254.37.204	3	0.00287081339713	8.44432472625
192.168.0.105	506	0.484210526316	1.04629365227
192.168.0.104	52	0.0497607655502	4.32884750883
169.254.255.255	10	0.00956937799043	6.70735913208
192.168.0.1	88	0.0842105263158	3.56985560833
192.168.0.101	30	0.0287081339713	5.12239663136
192.168.0.100	316	0.302392344498	1.72550647879
192.168.0.103	18	0.0172248803828	5.85936222553
192.168.0.102	22	0.0210526315789	5.56985560833

Entropía de la fuente
$H(S) = 1{,}99810125093$



En este caso la IP más consultada en la red fue la 192.168.0.105. Al igual que en el punto anterior por consecuencia de su alta probabilidad de aparecer en la fuente, su información no supera a la entropía que ofrece la red.