DEPARTAMENTO
DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

# Trabajo Práctico I

**Wiretapping**

Teoría de las Comunicaciones
Segundo Cuatrimestre de 2017


| Integrante | LU | Correo electrónico |
|---|---|---|
| Castiglione, Rubén Adrián | 818/15 | adriancastiglione@gmail.com |
| Sassone, Federico Sebastián | 602/13 | fede.sassone@hotmail.com |
| Rodriguez, Santiago Gabriel | 94/14 | santi_rodri_94@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

# 1. Introducción

El objetivo de este trabajo práctico es darnos un primer acercamiento al funcionamiento de las redes ën la vida real". Se nos dieron herramientas para capturar paquetes en redes públicas o privadas y con el contenido de las clases teóricas y prácticas, se espera que planteemos diferentes hipótesis sobre las distintas redes sniffeadas y tratemos de justificar sus comportamientos. Se espera que contestemos algunas preguntas planteadas en el enunciado y que elaboremos y busquemos respuesta a las que nos surjan.

# 2. Experimentos

## 2.1. Red 1

Análisis de S1:

Esta es una captura de la red labos-dc de la facultad. Se capturó en modo promiscuo mediante una conexión Wi-Fi. La captura fue de aldedor de 30mil paquetes, se capturaron los mismos durante quince minutos en los laboratorios, comenzando a las 19hs un día martes mientras que se dictaban clases en los alrededores. Luego se prosiguió a capturar durante otros quince minutos en las aulas del segundo piso, aún conectados a la misma red. Creemos que esta fuente debería ser la de mayor entropía, pues muchísimos dispositivos que pueden manejar distintos protocolos tienen acceso a la red y la transferencia de información no debería ser para nada constante

A continuación, los datos obtenidos:

```
Capturas/Fede_Facu_labos_wifi.pcap
```

| simbolo | probabilidad | informacion |
|---|---|---|
| ('unicast', 'Raw') | 0.320491856891 % | 8.28549658358 bits |
| ('unicast', 'LLC') | 1.57956700896 % | 5.98432704886 bits |
| ('unicast', 'ARP') | 0.150434953234 % | 9.37664447164 bits |
| ('unicast', 'IP') | 66.4431944535 % | 0.589806658079 bits |
| ('unicast', 'IPv6') | 6.97233304991 % | 3.84221470494 bits |
| ('broadcast', 'IP') | 16.2927595003 % | 2.61769712146 bits |
| ('broadcast', 'ARP') | 7.92399764537 % | 3.65762773825 bits |
| ('broadcast', 'LLC') | 0.31722153182 % | 8.30029358551 bits |

```
entropia muestral: 1.53762068956
entropia maxima:   3.0
```

Podemos ver que a diferencia de las demás capturas, la entropía de la muestra es considerablemente alta, alcanzando un 50 % de la máxima entropía posible. También podemos ver que las transferencias en broadcast alcanzan casi un 25 % del total. Esto puede significar que se están perdiendo las direcciones de los dispositivos o que los mismos están haciendo broadcast constantemente. En cualquiera de los casos, creemos que esto tiene que ver con una gran cantidad de nuevas conexiones creandose y desconectándose. Nuestros símbolos de unicast varían entre varios protocolos, siendo IP el que tiene mayor probabilidad entre todos ellos. El hecho de que el simbolo con menos información tenga una probabilidad tan baja puede significar que el host tiene poco peso en comparación con la cantidad de conexiones establecidas.

## 2.2. Red 2

Análisis de S1:

Esta es una red perteneciente al centro comercial Dot. Se capturó en modo promiscuo con una conexión wifi por antena. La cantidad de paquetes asciende hasta 36mil. La captura se efectuó durante veinte minutos a las 18hs con alrededor de cincuenta personas con acceso a la misma. Creemos que no había tantos de ellos conectados a la misma y que el tráfico de la misma no fue tan alto.

A continuación los datos obtenidos.

```
Capturas/Santi_dot_wifi_modo_promiscuo.pcap
```

| simbolo | probabilidad | informacion |
|---|---|---|
| ('unicast', 'EAPOL') | 0.0847318646477 % | 10.2048077615 bits |
| ('unicast', 'IP') | 96.2061990925 % | 0.0557982371505 bits |
| ('unicast', 'IPv6') | 2.2057617668 % | 5.50257920865 bits |
| ('broadcast', 'IP') | 0.945716940906 % | 6.72437584429 bits |
| ('unicast', 'ARP') | 0.196796588859 % | 8.98907907048 bits |
| ('broadcast', 'ARP') | 0.360793746242 % | 8.11460995257 bits |

```
entropia muestral: 0.294262643146
entropia maxima:   2.58496250072
```

Esta red es parecida a la siguiente, la diferencia con las demás es la presencia de un protocolo EAPOL que tras una pequeña búsqueda, descubrimos que se utiliza para autenticar usuarios. Tiene sentido, ya que esta es una red completamente abierta y debería tener medidas adicionales de seguridad. Nuevamente, el simbolo IP de unicast tiene mayor probabilidad que los demás y menor información. Creemos que este identifica al Host y que nuevamente es una conexión orientada a transferencia de Datos. Finalmente, la entropía de la muestra es muy baja en comparación a la máxima alcanzable.

## 2.3. Red 3

Análisis de S1:

Esta es una red perteneciente a un instituo educativo. Se capturó en modo promiscuo por un cable ethernet. La captura fue de alrededor de 150mil paquetes, se realizó durante algunas horas durante horario de clases en un día de semana con un tráfico mediano. Elegimos esta fuente pues se diferencia de las demás en la frecuencia de envío de paquetes y el destino de los mismos.

A continuación, los datos obtenidos:

```
Capturas/Adrian_labo_iac_cableado.pcap
```

| simbolo | probabilidad | informacion |
|---|---|---|
| ('unicast', 'ARP') | 0.407741230637 % | 7.93813043569 bits |
| ('unicast', 'IP') | 95.32560771 % | 0.0690642715855 bits |
| ('unicast', 'IPv6') | 1.34808225058 % | 6.21294766738 bits |
| ('broadcast', 'IP') | 0.370673846034 % | 8.07563395944 bits |
| ('broadcast', 'ARP') | 2.53423855788 % | 5.30230385232 bits |
| ('broadcast', 'LLC') | 0.0136564048539 % | 12.8381346457 bits |

```
entropia muestral: 0.348019131383
entropia maxima:   2.58496250072
```

Podemos ver que la cantidad de tráfico por broadcast es menor a un 3 % sobre el total de tráfico en la red. La entropía de la muestra se aleja de la máxima por un amplio margen, creemos que para que esta fuera máxima, la fuente tendría que tener simbolos con probabilidades más cercanas, y vemos que no es el caso, pues los simbolos con protocolo IP unicast ocupan alrededor de un 95 % de la muestra. Este simbolo en particular, parece ser distinguido entre los demás. Creemos que la red se usa principalmente para transmitir datos mediante este protocolo y finalmente añadimos que la alta probabilidad de obtenerlo está relacionada con la baja información que transmite.

## 2.4. Modelo de fuente de informacion nula

Como un primer aproximamiento propusimos como modelo de fuente de informacion nula distinguir a los host a partir de la informacion que tiene cada una de las ip nuestra hipotesis es que una ip con mucha informacion y baja probabilidad es mas facil distinguirla de, por ejemplo un router que va a tener baja informacion y alta probabilidad.