



**DEPARTAMENTO  
DE COMPUTACION**

Facultad de Ciencias Exactas y Naturales - UBA

# Trabajo Práctico Número 1

---

6 de Mayo de 2018

Teoría de las Comunicaciones

Integrante	LU	Correo electrónico
COMPLETAR	COMPLETAR	COMPLETAR
Balbachan, Alexis	994/12	alexisbalbachan@gmail.com
Gatti, Mathias	477/14	mathigatti@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>

# Índice

<b>0. Introducción</b>	<b>3</b>
<b>1. Metodología</b>	<b>4</b>
1.1. Herramientas . . . . .	4
1.2. Modelo de las fuentes . . . . .	4
1.2.1. S1 . . . . .	4
1.2.2. S2 . . . . .	4
1.2.3. Capturas . . . . .	4
<b>2. Resultados</b>	<b>6</b>
2.1. Resultados en la fuente S2 . . . . .	6
2.1.1. Análisis de Grafos . . . . .	6
2.1.1.1. Red Domiciliaria . . . . .	6
2.1.1.2. Starbucks . . . . .	6
2.1.1.3. Laboratorios del DC . . . . .	7
<b>3. Conclusión</b>	<b>9</b>
3.0.1. Red Domiciliaria . . . . .	9
3.0.2. Starbucks . . . . .	9
3.0.3. Laboratorio de Computación . . . . .	9

## 0. Introducción

Iniciamos este trabajo con el objetivo de aprender sobre el protocolo ARP y mas en general las redes de Internet y sus algoritmos de intercambio de paquetes.

A lo largo de este informe describiremos ciertos análisis que tendrán como objetivo el modelado de emisores de información y la posterior detección de símbolos destacados. A partir de esta metodología creemos que podremos identificar dispositivos claves en la red como por ejemplo el gateway. Nuestra hipótesis es que este tendrá destacará en el intercambio de paquetes who-has siendo de los que mas reciba y envíe.

# 1. Metodología

## 1.1. Herramientas

Para la captura de tráfico se utilizó el módulo de manipulación de paquetes *Scapy* para python, el cual provee una interfaz sencilla para nuestros requerimientos puntuales. *Scapy* permite la captura y posterior guardado de paquetes en una red, para luego ser filtrados, inspeccionados o manipulados con facilidad. Además, para incrementar la cantidad de paquetes vistos por un host, se activó el modo promiscuo o modo monitor en sus respectivas interfaces de red.

## 1.2. Modelo de las fuentes

### 1.2.1. S1

Dado el tráfico de capa 2 obtenido en cada captura, se modeló una fuente de memoria nula  $S1 = \{s_1, s_2, s_3, \dots, s_n\}$  donde cada  $s_i$  está formado por una tupla  $\langle \text{broadcast}|\text{unicast}, \text{protocolo capa 3} \rangle$ .

### 1.2.2. S2

Igualmente que S1, se modeló la fuente de memoria nula S2 con el objetivo utilizando sólo las direcciones IP dentro de paquetes de protocolo ARP con el objetivo de poder distinguir los hosts de cada red. En este caso se consideraron diversas opciones para el modelado de la fuente, donde cada  $s_i$  representaba las direcciones IP de los hosts, aunque su contabilización se regía por si la dirección aparecía en los campos:

- Fuente o Destino
- who-has Fuente
- who-has Destino
- is-at Fuente
- is-at Destino

### 1.2.3. Capturas

Se hicieron 3 capturas en redes diferentes de 10000 paquetes cada una:

- Red hogareña mediana, con aproximadamente 10 usuarios, se utilizó una interfaz ethernet.
- Red pública grande, en este caso se capturó mediante una interfaz wifi el tráfico del laboratorio de informática de la universidad.

- Red pública grande, también mediante la interfaz wifi, se capturó el tráfico en un Starbucks.

## 2. Resultados

### 2.1. Resultados en la fuente S2

#### 2.1.1. Análisis de Grafos

A partir de los paquetes que se intercambian en distintas redes vemos los grafos subyacentes a las mismas. En estos cada vértice representa una IP local y cada arista va del origen al destino de un paquete who-has del protocolo ARP.

##### 2.1.1.1. Red Domiciliaria

En este grafo los dos nodos con mayor grado son 192.168.1.1 con grado 7 y 192.168.1.112

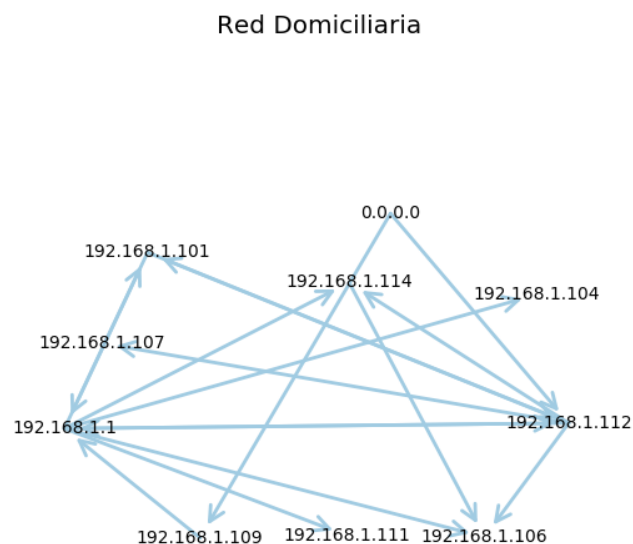


Figura 1

##### 2.1.1.2. Starbucks

Este grafo tiene solo dos nodos de los cuales el único que recibe paquetes es el nodo 172.19.96.1

Starbucks



Figura 2

### 2.1.1.3. Laboratorios del DC

Este grafo es mucho mas grande que los anteriores y cuenta con un nodo de máximo grado el cual es el 10.2.203.254.

8 / 9



### 3. Conclusión

Como resultado final pudimos identificar de distintas maneras nodos destacados, por ejemplo a partir del grafo subyacente que armamos pudimos identificar en todos los casos al gateway a partir del nodo de mayor grado. A continuación describimos brevemente cada caso analizado por separado.

#### 3.0.1. Red Domiciliaria

En la red domiciliaria se pudo ver en el grafo resultante como destacaban dos nodos. Uno de ellos, el de mayor grado, era el gateway, el otro creemos que fue la computadora que tomó las mediciones ya que estaba accediendo a multiples sitios de internet lo cual provoco un gran intercambio de paquetes.

#### 3.0.2. Starbucks

Quizas por una mala configuración de la red o por la poca clientela que había en este local en el horario en que se tomaron las mediciones (7:10 AM) es que este grafo resultó ser tan pobre, de todas maneras se pueden observar perfectamente los dos nodos que uno esperaría ver como minimo. El gateway y la computadora que tomo las mediciones.

#### 3.0.3. Laboratorio de Computación

Este es el grafo mas grande y en el cual se vuelve aún mas claro el patrón que veniamos viendo, el nodo 10.2.203.254 resalta completamente de los demás y concuerda perfectamente con nuestra hipótesis de que el gateway es el que mas paquetes intercambia en este protocolo, lo cual lo vuelve un nodo destacado.