# TP1: Wiretapping

Teoría de las Comunicaciones

Departamento de Computación
FCEN - UBA

03.09.2014

## 1. Introducción

En este taller vamos a abordar el desarrollo de tools de diagnóstico de red. El objetivo será analizar estadísticamente el protocolo ARP [1] y sacar algunas conclusiones acerca de los tipos de dispositivos de red que se pueden encontrar en un segumento de red determinado. Para ello, sugerimos el uso de dos herramientas modernas de manipulación y análisis de paquetes: Wireshark [2] y Scapy [3].

## 2. Normativa

- Fecha de entrega: 23.09.2014
- El informe deberá haber sido enviado por correo para esa fecha con el siguiente formato:
  to: tdc-doc at dc uba ar
  subject: debe tener el prefijo [tdc-wiretapping]
  body: nombres de los integrantes y las respectivas direcciones de correo electrónico
  attachment: el informe y el código desarrollado.

## 3. Enunciado

Cada grupo deberá resolver las consignas que siguen a continuación, tomando como referencia lo explicado en clase.

### 3.1. Primera consigna: capturando tráfico

(a) Implementar una *tool* para escuchar pasivamente en la red local.

(b) En base a los dos siguientes modelos de fuente de información propuestos:

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

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

- Adapte la *tool* del inciso (a) para estimar las probabilidades de dichas fuentes en función de los paquetes ARP observados y calcular la entropía de cada fuente.
- Usando dicha *tool*, realizar capturas de paquetes ARP sobre distintas LANs (una por cada integrante de grupo, mínimo 3). *En la medida de lo posible, intentar capturar en una red que no sea controlada (en el trabajo, en un shopping, etc.)*

### 3.2. Segunda consigna: gráficos y análisis

Utilizando lo hecho en la consigna previa, realizar un análisis que permita encontrar nodos distinguidos, valiéndose principalmente de gráficos. Sugerimos, entre otros, histogramas de IPs solicitadas o grafos dirigidos de IPs con pesos en los nodos (donde existirá un eje entre la IP $x$ y la IP $y$ sii se observó un request ARP con source IP $x$ y target IP $y$) y analizar que IPs son estadísticamente significativas en la LAN analizando la información de cada símbolo con respecto a la entropía de su respectiva fuente.

Se valorará especialmente en esta consigna la creatividad y el análisis propuesto. Recomendamos, pués, pensar cómo resultará más efectivo presentar la información recopilada.

## Referencias


[1] RFC 826 (ARP) `http://tools.ietf.org/html/rfc826`

[2] Wireshark (página web oficial) `http://www.wireshark.org`

[3] Scapy (página web oficial) `http://www.secdev.org/projects/scapy/`

[4] OUI (IEEE) `http://standards.ieee.org/develop/regauth/oui/oui.txt`