DEPARTAMENTO DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

TP1: Wiretapping

Fecha de entrega: 29 de Abril

Teoría de las Comunicaciones

Integrante	LU	Correo electrónico
Ignacio Gleria	387/10	igleria@dc.uba.ar
Patricio Mosse	515/06	patricio.mosse@gmail.com
David Temnyk	779/10	dtemnyk@dc.uba.ar
Gustavo Torrecilla	833/10	gustavo.d.t_90@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 hemos desarrollado una herramienta de diagnóstico de red con el objetivo de capturar los paquetes que se envían a través de la misma, identificar los distintos protocolos utilizados y principalmente, analizar el tráfico ARP (*Address Resolution Protocol*) mediante herramientas provistas por la teoría de la información. Este protocolo permite vincular identificadores de la capa de enlace (MAC) con direcciones de la capa de red (IP) de dispositivos conectados a una red local.

Hemos utilizado el lenguaje de programación Python para el desarrollo de la herramienta, valiéndonos principalmente del software de manipulación de paquetes Scapy. La captura de paquetes fue realizada sobre 4 redes que... **TODO:** Definir cuáles van a ser...

2. Desarrollo

Para analizar el tráfico en las redes, contamos con una fuente de información provista por la cátedra, que identifica los distintos tipos de paquetes capturados.

- $S = \{s_1...s_n\}$ siendo s_i el valor del campo *type* del frame de capa 2.

Adicionalmente, se nos pide que propongamos una fuente que nos permita distinguir nodos de una red en base al tráfico ARP. Por tal motivo, los símbolos de dicha fuente tendrían que estar conformados por campos de paquetes ARP.

Creemos que para poder distinguir nodos en una red es necesario obtener los campos $fuente$ y $destino$ de un paquete, ya que estos nos permiten identificar sobre qué nodos se concentra el tráfico ARP.

Dicho esto, la fuente propuesta es la siguiente:

- $S = \{s_1...s_n\}$ siendo s_i el valor del campo *source* y *destination* de los paquetes ARP.

Dadas estas fuentes, podemos obtener la *información* del evento "aparicion del símbolo s" de la siguiente manera:

$I(s) = -log(P(s))$, donde $I(s)$ representa la información obtenida con cada aparición del simbolo s, y $P(s)$ la probabilidad de aparición de un simbolo s.

Además, podemos calcular la *entropía* de una fuente obteniendo la esperanza de la información de los eventos, como se muestra a continuación:

$H(S) = \sum_{s \in S} P(s)I(s)$

3. Experimentación

3.1. Red Hogareña

En este experimento, capturamos los paquetes de la LAN de uno de los miembros de nuestro grupo. La medición fue realizada un día sábado desde las 12 hs hasta las 14 hs. La cantidad de paquetes capturados aproximadamente es de 125000. Sin embargo, sólo 153 de estos corresponden al protocolo ARP.

3.2. Red Mc Dondald's

Para el siguiente experimento, capturamos los paquetes de la LAN Wi-Fi del Mc Donald's ubicado en el shopping Alto Avellaneda. La medición fue realizada un día sábado desde las 18 hs hasta las 20 hs. La cantidad de paquetes capturados es de aproximadamente 65.000. De todos estos, sólo 918 corresponden al protocolo ARP.

3.3. Otra Red

3.4. Red Laboratorios DC

Para el último experimento, capturamos los paquetes de la LAN Wi-Fi Laboratorios-DC del Departamento de Computació de la FCEyN de la UBA. La medición fue realizada un día Lunes desde las 15hs y durante 15 minutos. La cantidad de paquetes capturados es de 19.000. De todos estos, sólo 974 corresponden al protocolo ARP.

3.4.1. Descripción

El siguiente experimento consistió en medir la LAN Wi-Fi pública del shopping Alto Palermo. Esta medición se llevó a cabo un día Sábado a las 21hs, con un tiempo de medición fue de aproximádamente 40 minutos y se capturaron 1569 paquetes ARP, de los cuales 687 eran de tipo *who-has*.

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*.

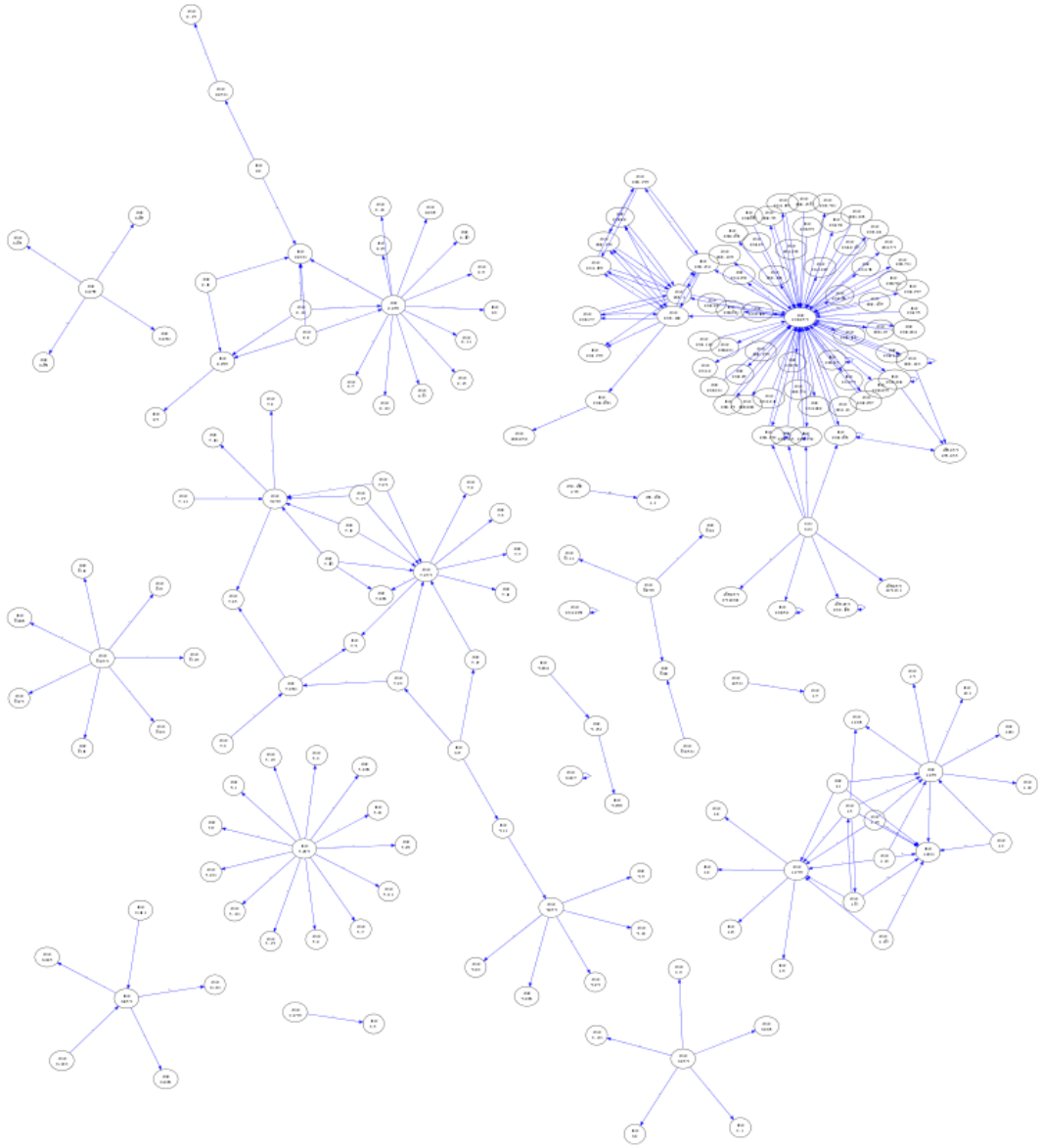

Figura 1: Grafo Medición DC

Como podemos ver en el grafo, la red tiene dos nodos que se destacan. Uno de estos nodos, el cual

tiene la dirección IP *117.17.12.1*, recibe muchos paquetes de la mayoría de los otros nodos de la red, pero no envía ninguno. Y el otro, con dirección IP *117.17.12.2* recibe varios paquetes y también envía varios.

También podemos observar que hay un nodo con dirección *0.0.0.0*, el cual envía varios mensajes.

3.4.2. Fuente: Destino

3.4.3. Fuente: Origen

3.4.4. Discusión

4. Discusión

5. Conclusión