DEPARTAMENTO DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

Trabajo Práctico Número 1

7 de Mayo de 2018 — Teoría de las Comunicaciones

Integrante	LU	Correo electrónico
COMPLETAR	COMPLETAR	COMPLETAR
COMPLETAR	COMPLETAR	COMPLETAR
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

0. Introducción

Intro Motivación Resumen (Objetivos) Hipotesis de trabajo

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 = $\{s_1, s_2, s_3, ..., s_n\}$ donde cada s_i está formado por una tupla <broadcast|unicast, protocolo capa 3>.

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 vertice 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

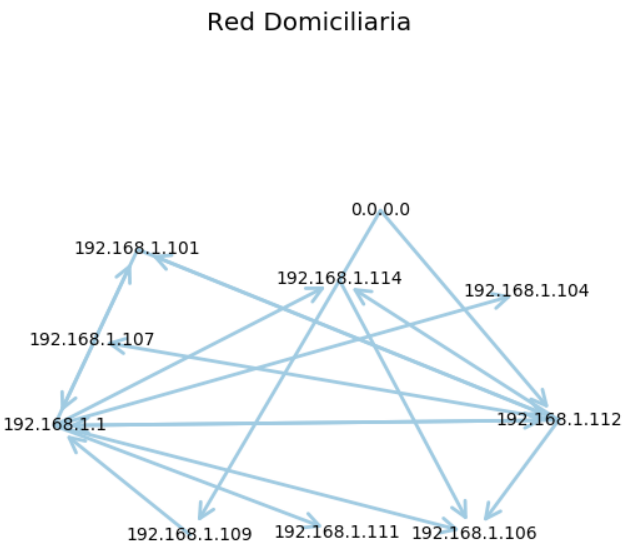

Figura 1

2.1.1.2. Starbucks

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

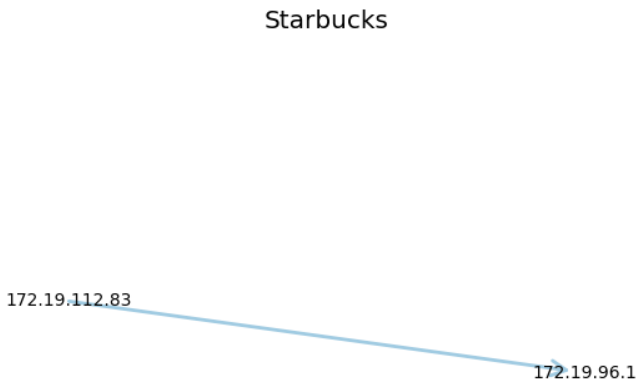

Figura 2

2.1.1.3. Laboratorios del DC

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

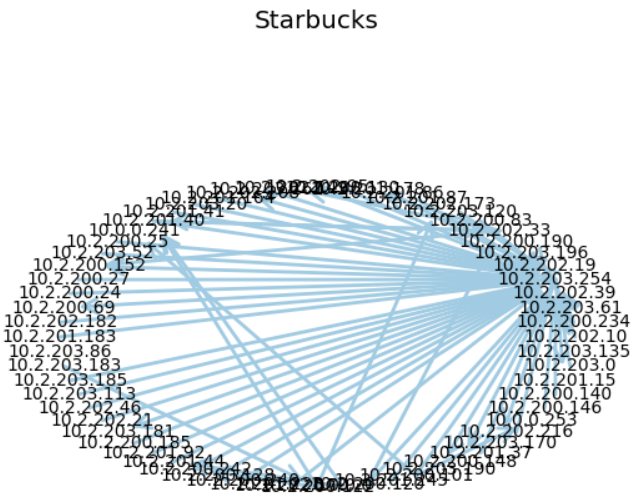
Starbucks
10.2.200.83
10.2.200.190
10.2.203.196
10.2.202.19
10.2.203.254
10.2.202.39
10.2.203.61
10.2.200.234
10.2.202.10
10.2.203.135
10.2.203.0
10.2.201.15
10.2.200.140
10.2.200.146
10.0.0.253
10.2.202.216
10.2.203.170
10.2.201.37
10.2.200.152
10.2.200.27
10.2.200.24
10.2.200.69
10.2.202.182
10.2.201.183
10.2.203.86
10.2.203.183
10.2.203.185
10.2.203.113
10.2.202.46
10.2.202.21
10.2.203.181
10.2.200.185

Figura 3

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 resulto 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 hipotesis de que el gateway es el que mas paquetes intercambia en este protocolo, lo cual lo vuelve un nodo destacado.