

Taller de Capa de Enlace

Teoría de las Comunicaciones

Departamento de Computación

FCEN - UBA

05.09.2012

1. Introducción

En este taller vamos a abordar en forma práctica algunas nociones de nivel de enlace, poniendo fundamentalmente el foco en el vínculo con la capa superior y desarrollando un acercamiento analítico. El objetivo será analizar de manera interactiva el protocolo ARP [1] y sacar algunas conclusiones de cómo se comportan los hosts en un segmento 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: 25.09.2012
- El código 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-enlace]
body: nombres de los integrantes y las respectivas direcciones de correo electrónico
attachment: el código fuente desarrollado.
- Se deberá entregar el informe impreso y abrochado con la lista de integrantes y los respectivos correos electrónicos (los mismos que fueran enviados por mail).

3. Enunciado

Cada grupo deberá resolver las consignas que siguen a continuación, tomando como referencia lo explicado en la clase de taller de la fecha que figura en el título.

3.1. Primera consigna: implementación de un cliente ARP

- (a) Implementar un cliente ARP sencillo: definir una función en Scapy (u otro lenguaje a elección con soporte para networking) que, dada una dirección IP, realice un pedido por la dirección física asociada y reciba y muestre la respuesta en caso de que ésta sea recibida.
- (b) Analizar qué ocurre al suministrarle distintas direcciones de la red local:
 - Una dirección inexistente,
 - La misma dirección de la máquina origen,
 - etc.

3.2. Segunda consigna: encontrando los vendedores

- (a) Implementar una función para escuchar pasivamente en la red local por un lapso de tiempo dado y capturar cada mensaje ARP encontrado.
- (b) A partir de lo anterior, obtener las direcciones físicas involucradas y exhibir los respectivos OUI (i.e., vendors). Para conseguir el mapeo de los bits de la MAC a cada vendor, recurrir a [4].

3.3. Tercera consigna: gráficos y análisis

Utilizando lo hecho en la consigna previa, graficar los datos encontrados y realizar un análisis de lo observado. Sugerimos, entre otros, histogramas de IPs solicitadas o grafos dirigidos de IPs (donde existirá un eje entre la IP x y la IP y si se observó un request ARP con source IP x y target IP y).

Se valorará especialmente en esta consigna la creatividad y el análisis propuesto. Recomendamos, pues, 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>