

**INSTITUTO POLITECNICO NACIONAL
ESCUELA SUPERIOR DE COMPUTO**

| | | |
|-------------------|------------------------------|---|
| Asignatura | Arquitectura de Computadoras | Realizó |
| Profesor | Miguel Ángel Alemán | López Jiménez Sonia Herrera Valdés Oswaldo |

| | |
|-------------|--|
| Tema | <i>Protocolo de resolución de direcciones (ARP)</i> |
|-------------|--|

PROTOCOLO DE RESOLUCIÓN DE DIRECCIONES “ARP”

ARP (Address Resolution Protocol) El protocolo ARP le permite a una maquina conocer la dirección física de una maquina destino en la misma red física, dada únicamente la dirección IP de la maquina destino.

Descripción del ataque ARP

- La maquina A quiere resolver la dirección IP de B.
- Petición ARP para pedir que la maquina responda dando a conocer su dirección física.
- Todas la maquinas, incluyendo a B reciben la petición.
- B reconoce su dirección IP y envía una respuesta conteniendo su dirección física.
- K envía a igualmente una respuesta conteniendo su propia dirección física, ocasionando que la respuesta enviada previamente por B se pierda.
- A utilizara entonces la dirección física de K para "comunicarse" con B.

Cada respuesta ARP a una petición ARP será procesada por el protocolo, por lo que la ultima respuesta recibida será tomada en cuenta por el solicitante. Como consecuencia la tabla de parejas dirección IP, dirección física) en la maquina A sea inconsistente. Lo único que resta por hacer es que K genere una petición ARP usando la dirección IP de A y su propia

dirección física para solicitar la dirección física de B. En el caso de B al recibir esta petición actualiza su tabla con la pareja y le envía a K la respuesta ARP.

Todo el trafico de A a B pasa por K y todo el trafico de B hacia A pasa también por K. La maquina K estará actuando como ruteador entre A y B dentro del mismo segmento.

Sintaxis:

```
Arp -s dir_inet dir_eth[dir_if]
```

```
Arp -d dir_inet [dir_if]
```

```
Arp -a [dir_inet][ -N dir_if]
```

Por ejemplo: ARP -a

Interfaz (ip de la maquina desde donde se hace el broadcast)

| Dirección ip | Dirección fisica(MAC) | Tipo de conexión |
|---------------|-----------------------|------------------|
| 192.168.0.100 | 40-F4-4D-7F-F3 | dinámico |

Gestión de tablas ARP

Las tablas ARP establecen enlaces entre las capas de protocolo y de 'link' (en caso de una red local Ethernet, sería entre dirección IP y dirección MAC). Cada host de una subred necesita conocer la dirección física de los demás para poder mandar paquetes a los destinatarios adecuados. Estas direcciones se almacenan en un caché ARP.

En caso de no conocer la dicha dirección MAC, se hace una petición de broadcast (por ejemplo cuando se enciende el equipo) que sería cómo "Hola ! Quién es la dirección IP w.x.y.z ?". La máquina con tal dirección IP contesta : "Yo soy la máquina w.x.y.z y mi MAC es 00:ad:f3:b1:22:4e". Entonces, nuestra máquina almacena esta MAC en su caché.

El Objeto 'neighbour' del comando ip gestiona el cache ARP. Estos son algunos ejemplos:

```
mrmime:~# ip neigh ls
192.168.2.5 dev eth0 lladdr 00:c0:ca:15:80:9c nud reachable
192.168.2.34 dev eth0 lladdr 00:05:1c:01:9d:c3 nud delay
```

```
192.168.2.72 dev eth0 lladdr 00:05:1c:01:6c:a9 nud reachable
192.168.2.1 dev eth0 lladdr 00:c0:ca:15:81:07 nud reachable
192.168.2.3 dev eth0 lladdr 00:01:02:ad:08:da nud stale
192.168.2.70 dev eth0 lladdr 00:40:f6:2c:27:13 nud reachable
192.168.2.21 dev eth0 lladdr 00:50:fc:42:07:b4 nud reachable
192.168.2.52 dev eth0 lladdr 00:05:1c:01:5e:1b nud delay
mrmime:~#
```

Puedo borrar una entrada:

```
mrmime:~# ip n d 192.168.2.52 dev eth0
mrmime:~# ip n l
192.168.2.5 dev eth0 lladdr 00:c0:ca:15:80:9c nud reachable
192.168.2.34 dev eth0 lladdr 00:05:1c:01:9d:c3 nud reachable
192.168.2.72 dev eth0 lladdr 00:05:1c:01:6c:a9 nud reachable
192.168.2.1 dev eth0 nud failed
192.168.2.3 dev eth0 lladdr 00:01:02:ad:08:da nud reachable
192.168.2.70 dev eth0 lladdr 00:40:f6:2c:27:13 nud reachable
192.168.2.21 dev eth0 lladdr 00:50:fc:42:07:b4 nud reachable
192.168.2.52 dev eth0 lladdr 00:05:1c:01:5e:1b nud reachable
```

Que paso ? Realmente la entrada correspondiente no desaparecerá de inmediato. Se quedara hasta que el último cliente que la usa la 'libere'

Los otros comandos para añadir o cambiar una entrada son:

- ip neigh add
- ip neigh change

Formato de Datagrama de ARP.

| | | | | |
|--------------------------|------|--------------------------|----|----|
| 0 | 8 | 16 | 24 | 31 |
| TIPO DE HARDWARE | | TIPO DE PROTOCOLO | | |
| HLEN | PLEN | OPERACION | | |
| SENDER HA (octeto 0 - 3) | | | | |
| SENDER HA (OCTETO 4 - 5) | | SENDER IP (OCTETO 0 - 1) | | |
| SENDER IP (OCTETO 2 - 3) | | TARGET HA (OCTETO 0 - 1) | | |
| TARGET HA (octeto 2 - 5) | | | | |
| TARGET IP (octeto 0 - 3) | | | | |

Formato de mensaje del ARP

| Campo | Descripción |
|------------|---|
| HLEN | Longitud de la dirección del hardware |
| PLEN | Longitud de la dirección del protocolo |
| Operación | Indica si es mensaje de consulta o de respuesta |
| HW Emisor | Dirección Física del Emisor |
| IP Emisor | Dirección IP del Emisor |
| HW Destino | Dirección Física del Destino |
| IP Destino | Dirección IP del Destino |

Seguridad y ARP

Al igual que ocurre con casi todos los protocolos de comunicaciones, y en concreto TCP/IP, el protocolo ARP puede ser usado por un posible atacante para objetivos no deseados.

Una de las técnicas más usadas en este sentido es la conocida como ARP Spoofing que, como su nombre indica, consiste en el uso del protocolo

para hacerse pasar por quién no se es en realidad, es decir, para suplantar a otra persona o máquina.

Básicamente consiste en enviar a la máquina objetivo del ataque un paquete con la dirección IP que queremos suplantar pero con la dirección física de nuestra tarjeta de red. En este caso, la máquina objetivo guardará la entrada ARP en su tabla caché, y a partir de ese momento todos los paquetes que envíe a la dirección IP suplantada llegarán a la máquina del atacante, y no a su legítimo destinatario. Este ataque dura aproximadamente unos 20 minutos (varía según el sistema operativo de la máquina atacada), que es el tiempo que se guardan las entradas en las tablas ARP.

La pregunta que ahora os haréis es: ¿Cómo podemos enviar a una máquina un paquete falseado?. Bien, pues existen diferentes programas circulando por Internet que precisamente hacen esto, como arp-fun, que son fácilmente asequibles a cualquiera que los busque.

Estos ataques es posible realizarlos solo en el caso de redes LAN, ya que en cuanto nos encontremos con conexiones dial-up (modems, por ejemplo) no existen tarjetas de red a las que redireccionar. Además, las nuevas tarjetas de red hacen una actualización de las tablas ARP caché en intervalos muy cortos (unos cinco minutos), por lo que el ataque es de duración muy limitada.

Existen también programas específicos para controlar estos ataques, como ARPwatch, que observan los cambios que se producen en las entradas IP/Ethernet, enviando un correo al administrador de la red si aprecian cambios incorrectos.

Las técnicas utilizadas para sniffear en redes conmutadas se basan en el conocido "ARP poison" (envenenamiento ARP). Este sencillo ataque consiste en mandar un paquete del tipo "REPLY ARP" en el que otorgamos a una IP una MAC distinta de la real. La mayoría de los S.O (excepto Linux 2.4 y Solaris 8) no implementan estados en el protocolo ARP y por tanto aceptan el REPLY aún sin haber realizado ninguna petición.

Usando esta técnica para sniffear las conexiones entre dos equipos "A" y "B", mandaremos al equipo "A" un "ARP REPLY" diciéndole que la MAC correspondiente a la ip de "B" es la del equipo donde está el sniffer. Seguidamente haremos la operación inversa con B y haremos un _mini_proxy entre A y B. De esta forma todas las comunicaciones entre A y B pasarán por nuestra máquina. Seguro que los más avisados pensaréis: "Pero si los switch's no soportan una MAC por dos puertos distintos". Eso es cierto, los switch's guardan una tabla con las MAC's visibles desde cada una de sus bocas. Pero esa caché tiene un tamaño limitado, ¿qué pasa si

la llenamos de entradas falsas? por lo general se vuelve a generar con la nueva información. También he oído comentar que los servidores DNS pueden envenenarse, esto nos daría la posibilidad de sniffear a través de Internet.

ARP Redirect

Las peticiones ARP tienen como dirección de origen la IP y MAC del emisor, para que el receptor no tenga que preguntarla cuando responda.

Los ordenadores, guardan esta información en su cache.

Sabiendo esto, podemos redirigir el tráfico de ordenadores cercanos, enviando tramas ARP indicando como dirección de origen nuestra dirección MAC y como IP de origen la del router, para hacer creer que somos el router, y nos envíen las tramas a nosotros.

También podemos hacer creer al switch que la dirección MAC del router es la nuestra, para que nos envíe todos los paquetes a enrutar, y luego nosotros se los mandaremos a la MAC verdadera del router.