

Problema 2

RMON y ARP

Reyes Ortega Ulises Axel
Garcia Ibañez Luis Arturo
Rosas Hernandez Oscar Andres

**¿Qué está
pasando?**



El internet de una ciudad presenta baja respuesta

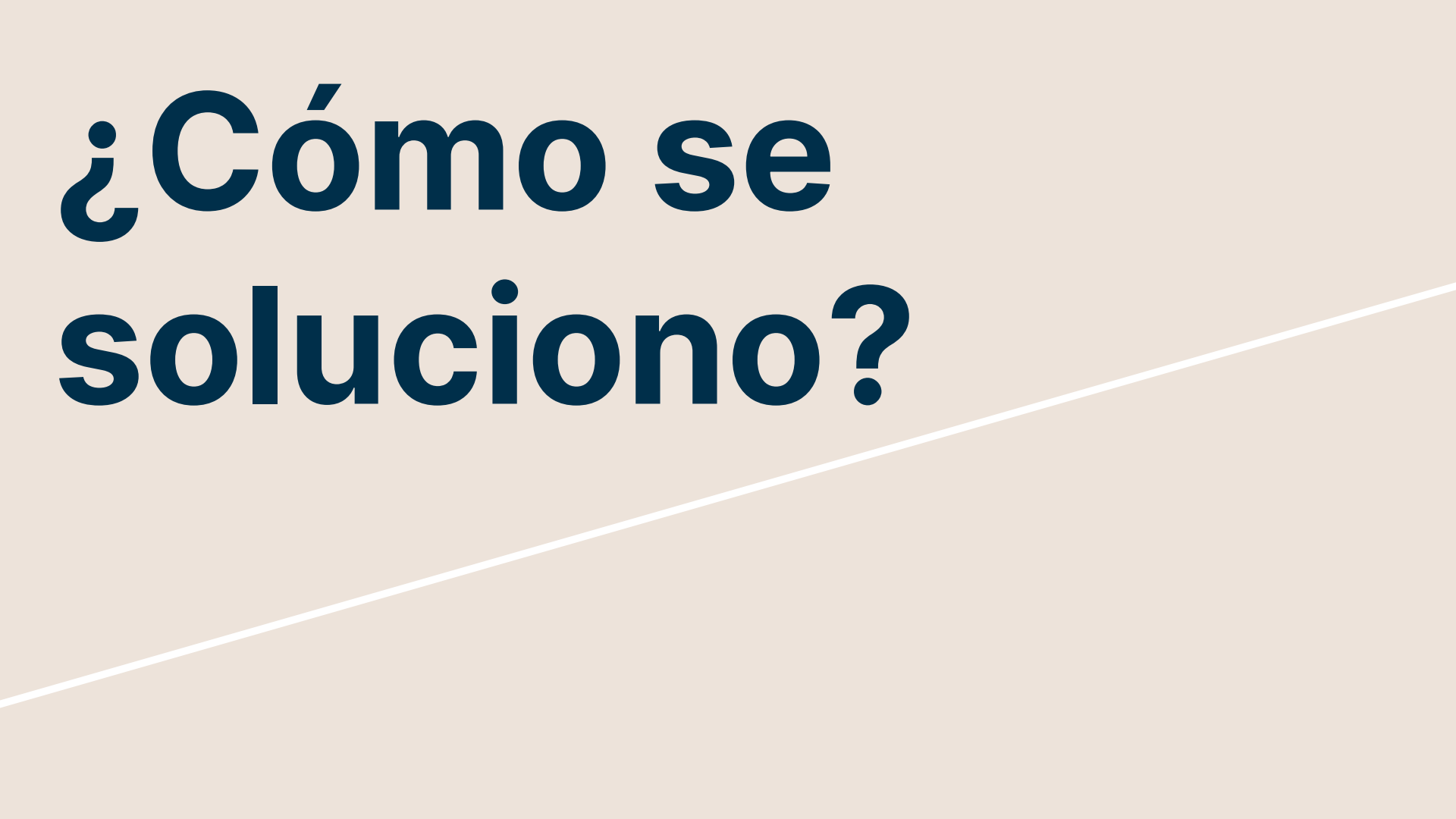
- **Pérdida de paquetes**
- **Problemas del hardware que reenvía**

Los usuarios denuncian problemas en el acceso a los servidores vía TCP/IP.

- **Perdida de Paquetes**
- **Parámetros incorrectos en los encabezados TCP/IP**
- **Restablecimiento del lado de la aplicación**

Eventualmente los problemas se resuelven reseteando los servidores, pero es una solución temporal pues los problemas se vuelven a presentar.

**¿Cómo se
soluciono?**



**Varias sondas RMON en
la red y detecta que el
tráfico de broadcast es el
40% del tráfico total de la
red**

**Se ponen filtros en las
sondas para solo
capturar el tráfico de
broadcast**

RMON

RMON admite la captura de paquetes (con filtros si se desea) y el envío de los paquetes capturados a un NMS (Network Management System) para su análisis.

Filtro de datos

Permite que se analice los paquetes observados sobre la base de un patrón de bits que coincida con una parte del paquete (o no coincidencia).

Los resultados son que
varios de los servidores
están enviando
solicitudes **ARP** de
manera ***anormal***

ARP: Address Resolution Protocol

El protocolo de resolución de direcciones es un protocolo de comunicaciones de la *capa de enlace de datos*, responsable de encontrar la dirección de hardware (MAC) que corresponde a una determinada dirección IP.

ARP: Address Resolution Protocol

Para ello se envía un paquete (ARP request) a la dirección de difusión de la red (broadcast, MAC = FF FF FF FF FF FF) que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina (u otra) responda (ARP reply) con la dirección Ethernet que le corresponde.

Cada máquina mantiene una caché con las direcciones traducidas para reducir el retardo y la carga.

ARP: Address Resolution Protocol

ARP permite a la dirección de Internet ser independiente de la dirección Ethernet.

De manera sencilla de explicar, el objetivo del protocolo ARP es permitir a un dispositivo conectado a una red LAN obtener la dirección MAC de otro dispositivo conectado a la misma red LAN cuya dirección IP es conocida.

Para realizar esta conversión, el nivel de enlace utiliza las tablas ARP, cada interfaz tiene tanto una dirección IP como una dirección física MAC.

Tablas ARP

Ejemplificando, para localizar a la persona "X" entre 150 personas: preguntar por su nombre a todos, y el señor "X" debe responder.

Cuando a A le llegue un mensaje con dirección origen IP y no tenga esa dirección en su caché de la tabla ARP, enviará su trama ARP a la dirección broadcast (física = FF:FF:FF:FF:FF:FF), con la IP de la que quiere conocer su dirección física. Entonces, el equipo cuya dirección IP coincida con la pregunta, responderá a A enviándole su dirección física.

En este momento, A ya puede agregar la entrada de esa IP a la caché de su tabla ARP.

Tablas ARP

Las entradas de la tabla se borran cada cierto tiempo, ya que las direcciones físicas de la red pueden cambiar.

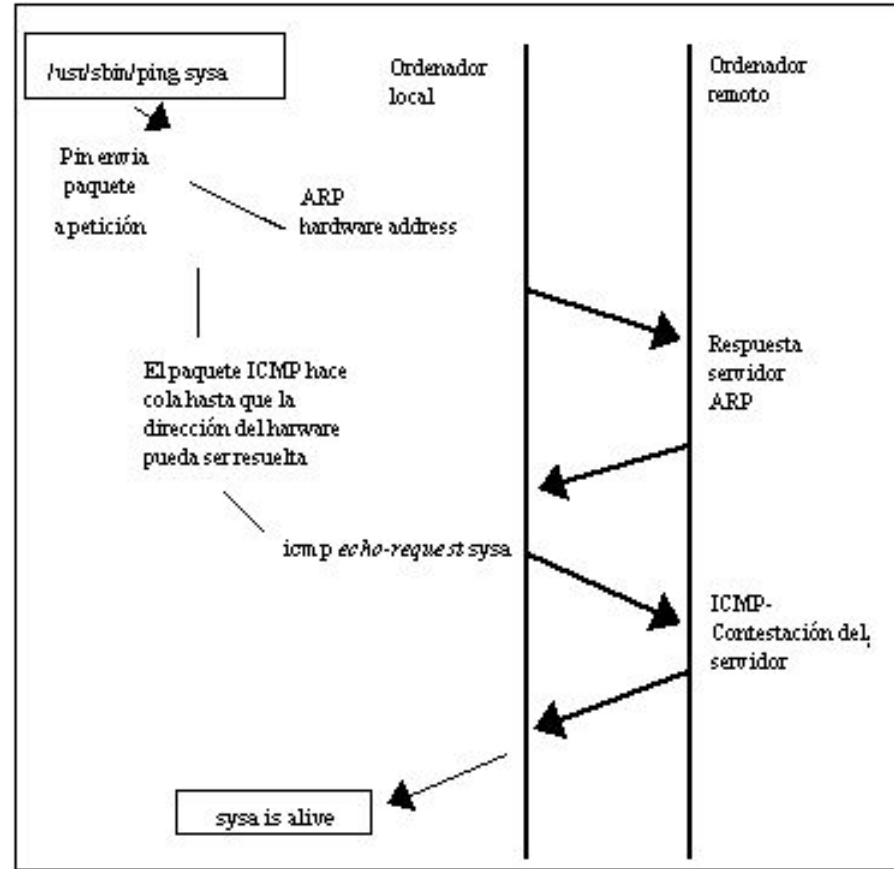
Por ejemplo si se estropea una tarjeta de red y hay que sustituirla, o simplemente algún usuario de la red cambia de dirección IP.

**Se usan ahora filtros
para capturar las
"conversaciones"
cliente / servidor**

**Se ve que las solicitudes
de información están
siendo respondidas; pero
no con una respuesta.
Si no con las solicitudes
ARP :c**

¿Cuándo se envía una solicitud ARP?

Las solicitudes ARP son realizadas cuando se intenta mandar un mensaje a una IP cuya dirección MAC es desconocida.



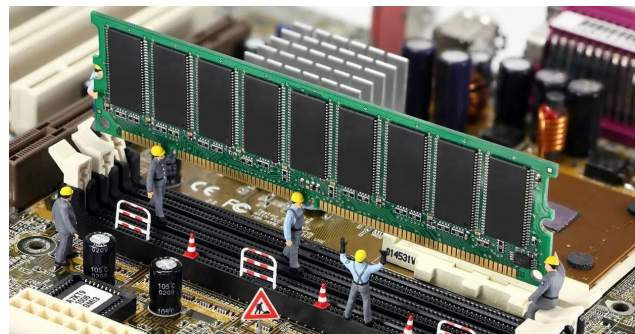
**Se evidencia que el servidor
pierde la información de las
direcciones físicas de los clientes
en cuanto las obtiene, es decir, su
cache ARP se limpia
constantemente.**

Posibles escenarios

Configuración del Servidor



Falla de hardware(RAM)



Al revisar la configuración del servidor se encontró que su valor de time out de la caché estaba fijada en milisegundos en vez de minutos.



Time out



El Time out de la tabla ARP es la cantidad de tiempo que el servidor mantiene las asignaciones de direcciones IP-MAC en su caché ARP para adaptarse a su entorno.

- **Tiene un valor por defecto.**
- **Un time out de 0 nunca borra el cache.**

Time out - Posible motivo

Ejemplo Servidor Cisco:

```
R1#show ip arp
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	13.13.13.1	-	ca00.0a74.0008	ARPA	FastEthernet0/0
Internet	13.13.13.3	97	ca02.0a74.0008	ARPA	FastEthernet0/0
Internet	15.15.15.1	-	ca00.0a74.0006	ARPA	FastEthernet0/1
Internet	15.15.15.5	136	ca04.0a74.0008	ARPA	FastEthernet0/1

```
!-- setting the timeout for 10 seconds
```

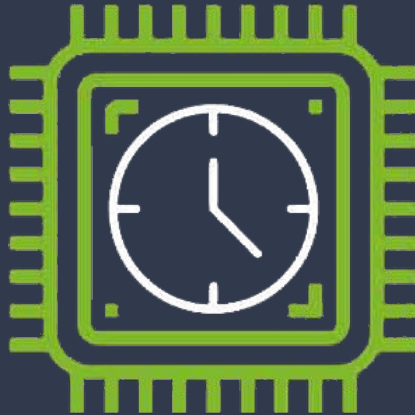
```
R1(config-if)#int f0/0
```

```
R1(config-if)#arp timeout 10
```

Formato: arp timeout <x> seconds.



**El problema se resolvió
completamente cambiando el
valor del timeout de la caché.**



A considerar

Se debería dar un manual de instrucciones del servidor donde se especifique el tipo de unidad de tiempo que utilizan los comandos.



Gracias por
su atención
:)

