El muestreo de la red ha detectada un alto índice de pedidos de dirección por parte del dispositivo con IP 192.168.0.1, el cual contactó a varios dispositivos en múltiples ocasiones en el tiempo en que se tomó monitorio la red. Puntualmente, se destacó el dispositivo con la IP 192.168.0.107, en donde hubo 180 solicitudes, contra una 6 solicitudes por parte del 192.168.0.107 al 192.168.0.1.

Por otro lado los dispositivos con la IP 192.168.0.106 y 192.168.0.108 enviaron una alta cantidad de solicitudes al 192.168.0.1 (respecto a la media).

Viendo esto, podemos decir que el dispositivo con IP 192.168.0.1 es un nodo importante en la red, probablemente un ruter. Se puede deducir que durante un periodo prolongado el dispositivo 192.168.0.107 estuvo extrayendo información del nodo, lo cual explicaría por qué existe un trafico de paquetes más elevado desde el nodo hasta el 192.168.0.107 que desde este último al nodo.

En el caso del dispositivo con IP 192.168.0.106, y 192.168.0.108 las solicitudes para buscar al nodo podrían deberse a que estos estaban enviando información al nodo.

La mayoría de los dispositivos contenía una IP que contenía el prefijo de 192.168.0, con lo cual se puede deducir que esta es la IP de la red analizada. Además, se han detectado paquetes provenientes de redes privadas distintas (puntualmente de dos dispositivos).

Se registró un trafico mínimo entre dispositivos en donde el 192.168.0.1 no estaba involucrado.

Se han interceptado paquetes ARP cuya función desconocemos. Se registraron casos de dispositivos que enviaban paquetes a su propio IP. Además, se detectó una alta densidad paquetes ARP que provenían de dispositivos con una IP 0.0.0.0. Se ha creado un registro que omite dichos paquetes para tener una versión menos distorsionada por dicho evento. Además, se han detectado paquetes con 255.255.255.255 como IP de origen y destino, lo cual no es una IP válida.