

HI

Summarize, what is happening here?

00:56:26.347372 ARP, Request who-has 192.168.47.164 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.347410 ARP, Request who-has 192.168.47.165 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.347449 ARP, Request who-has 192.168.47.166 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.347487 ARP, Request who-has 192.168.47.167 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.347526 ARP, Request who-has 192.168.47.168 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.347565 ARP, Request who-has 192.168.47.169 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.347603 ARP, Request who-has 192.168.47.170 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.347641 ARP, Announcement 192.168.47.171 (Broadcast), length 28  
00:56:26.347680 ARP, Request who-has 192.168.47.172 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.347719 ARP, Request who-has 192.168.47.173 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.347765 ARP, Request who-has 192.168.47.174 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.347804 ARP, Request who-has 192.168.47.175 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.347843 ARP, Request who-has 192.168.47.176 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.347881 ARP, Request who-has 192.168.47.177 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.347919 ARP, Request who-has 192.168.47.178 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.347958 ARP, Request who-has 192.168.47.179 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.347997 ARP, Request who-has 192.168.47.180 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.348035 ARP, Request who-has 192.168.47.181 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.348073 ARP, Request who-has 192.168.47.182 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.348112 ARP, Request who-has 192.168.47.183 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.348150 ARP, Request who-has 192.168.47.184 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.348188 ARP, Request who-has 192.168.47.185 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.348235 ARP, Request who-has 192.168.47.186 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.348274 ARP, Request who-has 192.168.47.187 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.348312 ARP, Request who-has 192.168.47.188 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.348351 ARP, Request who-has 192.168.47.189 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.348389 ARP, Request who-has 192.168.47.190 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.348428 ARP, Request who-has 192.168.47.191 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.348466 ARP, Request who-has 192.168.47.192 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.348505 ARP, Request who-has 192.168.47.193 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.348543 ARP, Request who-has 192.168.47.194 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.348581 ARP, Request who-has 192.168.47.195 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.348620 ARP, Request who-has 192.168.47.196 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.348658 ARP, Request who-has 192.168.47.197 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.348697 ARP, Request who-has 192.168.47.198 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.348744 ARP, Request who-has 192.168.47.199 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.348782 ARP, Request who-has 192.168.47.200 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.348821 ARP, Request who-has 192.168.47.201 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.348860 ARP, Reply 192.168.47.200 is-at 00:0c:29:0f:71:a3 (oui Unknown), length 46  
00:56:26.348876 ARP, Request who-has 192.168.47.202 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.348914 ARP, Request who-has 192.168.47.203 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.348953 ARP, Request who-has 192.168.47.204 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.348991 ARP, Request who-has 192.168.47.205 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.349030 ARP, Request who-has 192.168.47.206 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.349068 ARP, Request who-has 192.168.47.207 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.349106 ARP, Request who-has 192.168.47.208 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.349145 ARP, Request who-has 192.168.47.209 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.349183 ARP, Request who-has 192.168.47.210 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.349222 ARP, Request who-has 192.168.47.211 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.349268 ARP, Request who-has 192.168.47.212 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.349307 ARP, Request who-has 192.168.47.213 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.349346 ARP, Request who-has 192.168.47.214 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.349384 ARP, Request who-has 192.168.47.215 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.349422 ARP, Request who-has 192.168.47.216 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.349460 ARP, Request who-has 192.168.47.217 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.349499 ARP, Request who-has 192.168.47.218 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.349537 ARP, Request who-has 192.168.47.219 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.349575 ARP, Request who-has 192.168.47.220 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.349613 ARP, Request who-has 192.168.47.221 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.349651 ARP, Request who-has 192.168.47.222 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.349690 ARP, Request who-has 192.168.47.223 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.349736 ARP, Request who-has 192.168.47.224 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.349775 ARP, Request who-has 192.168.47.225 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.349813 ARP, Request who-has 192.168.47.226 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.349851 ARP, Request who-has 192.168.47.227 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.349889 ARP, Request who-has 192.168.47.228 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.349928 ARP, Request who-has 192.168.47.229 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.349966 ARP, Request who-has 192.168.47.230 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.350004 ARP, Request who-has 192.168.47.231 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.350043 ARP, Request who-has 192.168.47.232 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.350081 ARP, Request who-has 192.168.47.233 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.350119 ARP, Request who-has 192.168.47.234 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.350158 ARP, Request who-has 192.168.47.235 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.350196 ARP, Request who-has 192.168.47.236 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.350243 ARP, Request who-has 192.168.47.237 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.350282 ARP, Request who-has 192.168.47.238 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.350323 ARP, Request who-has 192.168.47.239 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.350375 ARP, Request who-has 192.168.47.240 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.350416 ARP, Request who-has 192.168.47.241 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.350456 ARP, Request who-has 192.168.47.242 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.350496 ARP, Request who-has 192.168.47.243 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.350537 ARP, Request who-has 192.168.47.244 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.350577 ARP, Request who-has 192.168.47.245 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.350618 ARP, Request who-has 192.168.47.246 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.350658 ARP, Request who-has 192.168.47.247 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.350699 ARP, Request who-has 192.168.47.248 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.350747 ARP, Request who-has 192.168.47.249 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.350788 ARP, Request who-has 192.168.47.250 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.350829 ARP, Request who-has 192.168.47.251 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.350869 ARP, Request who-has 192.168.47.252 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.350909 ARP, Request who-has 192.168.47.253 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.350950 ARP, Request who-has 192.168.47.254 (Broadcast) tell 192.168.47.171, length 28  
00:56:26.351000 ARP, Reply 192.168.47.254 is-at 00:50:56:f9:f5:54 (oui Unknown), length 46  
00:56:29.446972 ARP, Reply 192.168.47.1 is-at 00:0c:29:1d:b3:b1 (oui Unknown), length 28  
00:56:29.447023 ARP, Reply 192.168.47.2 is-at 00:0c:29:1d:b3:b1 (oui Unknown), length 28  
00:56:29.447073 ARP, Reply 192.168.47.200 is-at 00:0c:29:1d:b3:b1 (oui Unknown), length 28  
00:56:29.447131 ARP, Reply 192.168.47.2 is-at 00:0c:29:1d:b3:b1 (oui Unknown), length 28  
00:56:29.447166 ARP, Reply 192.168.47.254 is-at 00:0c:29:1d:b3:b1 (oui Unknown), length 28  
00:56:29.447198 ARP, Reply 192.168.47.2 is-at 00:0c:29:1d:b3:b1 (oui Unknown), length 28  
00:56:31.933090 ARP, Reply 192.168.47.1 is-at 00:0c:29:1d:b3:b1 (oui Unknown), length 28  
00:56:31.933204 ARP, Reply 192.168.47.2 is-at 00:0c:29:1d:b3:b1 (oui Unknown), length 28  
00:56:31.933319 ARP, Reply 192.168.47.200 is-at 00:0c:29:1d:b3:b1 (oui Unknown), length 28  
00:56:31.933414 ARP, Reply 192.168.47.2 is-at 00:0c:29:1d:b3:b1 (oui Unknown), length 28  
00:56:31.933499 ARP, Reply 192.168.47.254 is-at 00:0c:29:1d:b3:b1 (oui Unknown), length 28  
00:56:31.933584 ARP, Reply 192.168.47.2 is-at 00:0c:29:1d:b3:b1 (oui Unknown), length 28



In this text, a device with the IP address 192.168.47.171 is sending ARP (Address Resolution Protocol) requests to identify the MAC (Media Access Control) addresses associated with a range of IP addresses (192.168.47.164 to 192.168.47.247) within its local network. It sends broadcast messages asking "who-has" each IP address, and a reply is received from the device with IP address 192.168.47.200, providing its MAC address (00:0c:29:0f:71:a3).

HI

Anything suspicious?



Based on the provided log, there isn't anything inherently suspicious. The log shows a series of Address Resolution Protocol (ARP) requests originating from the IP address 192.168.47.171. These requests are attempting to find the MAC addresses associated with various IP addresses in the local network, which is a typical function of ARP.

However, it is important to consider the context in which this activity is occurring. If this is normal behavior for your network and is expected, then there is likely nothing to worry about. On the other hand, if this activity is unexpected, it could potentially indicate an issue such as an unauthorized device on the network or a device attempting to discover other devices for malicious purposes.

To determine if there is any cause for concern, it is recommended to analyze the network traffic patterns and compare them to normal behavior, as well as to verify the devices on the network to ensure they are all authorized.

HI

Isn't it odd that a lot of ARP replies have the MAC address 00:0c:29:1d:b3:b1 for a variety of IP addresses?



Yes, you are correct. It is unusual for multiple IP addresses to be associated with a single MAC address in ARP replies. This could potentially indicate an issue or malicious activity on your network. Some possible explanations for this behavior include:

- ARP Spoofing (ARP Poisoning): An attacker may be trying to intercept or manipulate network traffic by associating their MAC address with multiple IP addresses on the network. This would allow them to receive traffic intended for other devices and potentially launch man-in-the-middle attacks.
- Network Misconfiguration: It is possible that there is a misconfiguration on the network that is causing the same MAC address to be associated with multiple IP addresses. This could occur if multiple devices are using the same MAC address, or if a single device is incorrectly configured with multiple IP addresses.
- Virtualization: If you are using virtual machines on your network, it is possible that the same MAC address is being used for multiple virtual network interfaces. This could lead to the appearance of the same MAC address being associated with multiple IP addresses.

To determine the cause of this issue and take appropriate action, it is recommended to investigate further by analyzing the network traffic, reviewing the configurations of devices on the network, and potentially employing network monitoring tools to identify any anomalies or malicious activities.