arping

context

dit document geeft wat uitleg over arping

context

- ping: L3 van netwerk
- arping: L2 van netwerk.
- ping request kunnen gedropt, gefilterd worden door de host die de ICMP request ontvangt.
- arping stuurt een ARP request: '"Who has <IP>?"
- antwoord. "<IP> is at XX:XX:XX:XX:XX:XX" betekent dat deze hosts met mekaar kunnen communiceren.

voorbeeld

- firewall throttles ICMP request en beantwoord slechts 1/10 requests

```
root@backup:/var/lib/jellyfin# tcpdump -i enp4s0 host 10.11.12.14 and icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp4s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:43:54.649344 IP 10.11.12.6 > 10.11.12.14: ICMP echo request, id 26322, seq 21, length 64
23:43:55.673396 IP 10.11.12.6 > 10.11.12.14: ICMP echo request, id 26322, seq 22, length 64
23:43:56.697329 IP 10.11.12.6 > 10.11.12.14: ICMP echo request, id 26322, seq 23, length 64
23:43:57.721361 IP 10.11.12.6 > 10.11.12.14: ICMP echo request, id 26322, seq 24, length 64
23:43:58.745296 IP 10.11.12.6 > 10.11.12.14: ICMP echo request, id 26322, seq 25, length 64
23:43:59.769355 IP 10.11.12.6 > 10.11.12.14: ICMP echo request, id 26322, seq 26, length 64
23:43:59.769480 IP 10.11.12.14 > 10.11.12.6: ICMP echo reply, id 26322, seq 26, length 64
23:44:00.797389 IP 10.11.12.6 > 10.11.12.14: ICMP echo request, id 26322, seq 27, length 64
23:44:00.797556 IP 10.11.12.14 > 10.11.12.6: ICMP echo reply, id 26322, seq 27, length 64
23:44:01.817352 IP 10.11.12.6 > 10.11.12.14: ICMP echo request, id 26322, seq 28, length 64
23:44:02.841317 IP 10.11.12.6 > 10.11.12.14: ICMP echo request, id 26322, seq 29, length 64
23:44:03.865333 IP 10.11.12.6 > 10.11.12.14: ICMP echo request, id 26322, seq 30, length 64
23:44:04.889337 IP 10.11.12.6 > 10.11.12.14: ICMP echo request, id 26322, seq 31, length 64
23:44:05.913346 IP 10.11.12.6 > 10.11.12.14: ICMP echo request, id 26322, seq 32, length 64
23:44:06.937586 IP 10.11.12.6 > 10.11.12.14: ICMP echo request, id 26322, seq 33, length 64
23:44:07.961321 IP 10.11.12.6 > 10.11.12.14: ICMP echo request, id 26322, seq 34, length 64
23:44:08.985316 IP 10.11.12.6 > 10.11.12.14: ICMP echo request, id 26322, seq 35, length 64
23:44:10.009314 IP 10.11.12.6 > 10.11.12.14: ICMP echo request, id 26322, seq 36, length 64
```

- arping naar die firewall toont dat er verbinding mogelijk is.

```
root@backup:~# arping 10.11.12.14
ARPING 10.11.12.14
60 bytes from 70:4f:57:1e:c9:24 (10.11.12.14): index=0 time=331.923 usec
60 bytes from 70:4f:57:1e:c9:24 (10.11.12.14): index=1 time=324.411 usec
60 bytes from 70:4f:57:1e:c9:24 (10.11.12.14): index=2 time=318.760 usec
60 bytes from 70:4f:57:1e:c9:24 (10.11.12.14): index=3 time=303.412 usec
60 bytes from 70:4f:57:1e:c9:24 (10.11.12.14): index=4 time=314.296 usec
60 bytes from 70:4f:57:1e:c9:24 (10.11.12.14): index=5 time=370.946 usec
60 bytes from 70:4f:57:1e:c9:24 (10.11.12.14): index=6 time=309.831 usec
60 bytes from 70:4f:57:1e:c9:24 (10.11.12.14): index=7 time=295.216 usec
^C
```

meer info

- TCPdump primer
- arping primer

Linux