[Утилита arp-scan. Сканирование локальной сети с хоста.]

Category: GNU/Linux, arp-scan, cli commands, ip, mac, утилиты
2024-09-15

Введение.

Иногда возникает необходимость узнать какие устройства подключены к локальной сети. Это может понадобиться если вы хотите подключиться к одному из хостов и не помните его адрес или хотите убедиться в безопасности вашей сети и найти все скрытые устройства.

Как выполнить ARP сканирование локальной сети?

У всех устройств в сети есть **IP-адреса**. Для преобразования физических **MAC-адресов**, в **IP-адрес** используется протокол **ARP (Address Resolution Protocol)** — протокол разрешения адресов.

Когда хосту нужно обратиться к другому хосту в локальной сети, он отправляет специальный запрос в котором буквально спрашивает «У кого IP адрес 192.168.1.10«, хост с таким **IP-адресом** отправляет ответ «У меня, я 01-23-45-67-89-AB«, в ответе он передает свой физический **MAC-адрес** в этой сети. Дальше этот адрес заносится в специальную **ARP-таблицу**.

Формат сообщений ARP.

Формат сообщений **ARP** — простой. Сообщение содержит либо запрос с **IP-адресом**, либо ответ. Размер сообщения зависит от используемого сетевого протокола **IPv4** или **IPv6**, типа оборудования сети и так далее. Типы и размеры адресов определяются в заголовке сообщения. Заголовок завершается кодом сообщения. Код 1 для запроса и 2 для ответа. Тело сообщения состоит из четырех адресов, аппаратные и сетевые адреса отправителя и получателя.

Если в вашей сети есть устройства, которые не отвечают на любые запросы, такие как **Ping**, **HTTP**, **HTTPS** и так далее, то их можно найти послав **ARP-запрос**. Это могут быть различные **firewall** и маршрутизаторы. В таком случае **ARP** сканирование сети с хоста **GNU\Linux** будет единственным способом найти такое устройство.

Утилита ARP Scan.

ARP Scan или еще называемый **MAC Scanner** — это очень быстрый инструмент для сканирования локальной сети с хоста **GNU\Linux** с помощью **ARP**. Утилита показывает все **IPv4-адреса** устройств в вашей сети. Поскольку **ARP** не использует маршрутизацию, то такой вид сканирования работает только в локальной сети.

ARP Scan находит все активные устройства, даже если у них включен брандмауэр. Хосты не могут скрыться от **ARP** также как они скрываются от **ping**.

ARP сканирование не подходит для поиска хостов за пределами локальной сети, в таких ситуациях используйте **ping** сканирование.

Установка ARP Scan.

Этот **arp-сканер** сети доступен большинства GNU\Linux систем.

Для установки в **Debian** выполните:

```
$ sudo apt install -y arp-scan
```

Для установки в **Fedora** выполните:

```
$ sudo dnf -y install arp-scan
```

Сканирование сети.

ARP Scan позволяет находить активные хосты как в проводных сетях **Ethernet**, так и в беспроводных **Wi-Fi** сетях. Также есть возможность работать с **Token Ring** и **FDDI**. Не поддерживаются последовательные соединения **PPP** и **SLIP**, поскольку в них не используется **ARP**. Программу нужно запускать с правами суперпользователя.

Сначала надо узнать сетевой интерфейс, который используется для подключения к сети.

Для этого можно воспользоваться программой ip:

```
$ sudo ip addr list
```

Ответ:

```
hamster@pbs:~$ sudo ip addr list
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 74:d4:35:13:e9:ac brd ff:ff:ff:ff:ff:ff
    inet 100.67.99.10/24 scope global enp2s0
       valid_lft forever preferred_lft forever
    inet6 fe80::76d4:35ff:fe13:e9ac/64 scope link
       valid_lft forever preferred_lft forever
hamster@pbs:~$
```

В данном случае, это enp2s0.

Самый простой способ выполнить **ARP** сканирование и обнаружить все подключенные к локальной сети хосты – запустить программу со следующими параметрами:

sudo arp-scan --interface=enp2s0 --localnet

Ответ:

```
hamster@pbs:~$ sudo arp-scan --interface=enp2s0 --localnet
Interface: enp2s0, type: EN10MB, MAC: 74:d4:35:13:e9:ac, IPv4: 100.67.99.10
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
100.67.99.1     b8:69:f4:c2:a5:44       (Unknown)
100.67.99.8     c8:d9:d2:8a:39:1c       (Unknown)
100.67.99.11    c8:5a:cf:b1:28:06       (Unknown)
100.67.99.12    c0:3f:d5:07:a1:aa       (Unknown)
100.67.99.15    bc:24:11:25:fc:a5       (Unknown)
100.67.99.22    e8:40:f2:99:90:de       (Unknown)
100.67.99.254   e8:40:f2:99:90:de       (Unknown)

9 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.790 seconds (143.02 hosts/sec). 7 responded
hamster@pbs:~$
```

Здесь параметр --interface, задает интерфейс для сканирования, а --localnet, говорит, что нужно использовать все возможные **IP-адреса** для текущей сети.

Первый параметр можно опустить, тогда программа будет искать все узлы для интерфейса с меньшим номером в системе. В нашем примере имя интерфейса – enp2s0.

Вместо параметра --localnet, можно указать маску сети:

$ sudo arp-scan --interface=enp2s0 100.67.99.0/24

Ответ:

```
hamster@pbs:~$ sudo arp-scan --interface=enp2s0 100.67.99.0/24
Interface: enp2s0, type: EN10MB, MAC: 74:d4:35:13:e9:ac, IPv4: 100.67.99.10
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
100.67.99.1     b8:69:f4:c2:a5:44       (Unknown)
100.67.99.8     c8:d9:d2:8a:39:1c       (Unknown)
100.67.99.11    c8:5a:cf:b1:28:06       (Unknown)
100.67.99.12    c0:3f:d5:07:a1:aa       (Unknown)
100.67.99.15    bc:24:11:25:fc:a5       (Unknown)
100.67.99.22    e8:40:f2:99:90:de       (Unknown)
100.67.99.254   e8:40:f2:99:90:de       (Unknown)

11 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.790 seconds (143.02 hosts/sec). 7 responded
hamster@pbs:~$
```

ARP сканирование можно использовать, даже если у вашего интерфейса нет **IP-адреса**. Тогда в качестве исходящего адреса будет использован 0.0.0.0. Правда, на такие запросы могут ответить не все системы. Тогда **ARP** сканер сети не так эффективен.

ARP спуфинг и ARP прокси.

Поскольку в **ARP** нет поддержки аутентификации, **ARP** ответ на запрос может отправить любая машина, даже не та которой он был адресован. Иногда такое поведение используется в архитектуре сети — **ARP** прокси или маршрутизатор предает свой **IP-адрес** вместо адреса запрашиваемой машины. Это также может использоваться для перехвата данных, отправляемых хостом. Хакер может использовать **ARP** чтобы выполнить атаку «Человек посередине» или «Отказ в обслуживании» на других пользователей сети. Для защиты от таких атак существует специальное программное обеспечение.

Оригиналы источников информации.

1. losst.pro — ARP сканирование локальной сети Linux.