arp-scan

Arp-Scan的使用注意事项:

arp-scan可用来发现本地网络上的IP主机。它可以发现的所有主机，包括那些已经阻止所有IP访问，如已经打开防火墙和系统入口过滤器的主机。

arp-scan适用于以太网和802.11无线网络。它也可以与令牌环网和FDDI工作，但他们并没有经过测试。它不支持串行链路如PPP或SLIP，因为ARP不支持他们。

运行arp-scan需要root权限，或arp-scan必须是SUID root。因为它使用的读取和写入的以太网数据包的功能需要root权限。

发现本地网络上的所有主机

arp协议

ARP（地址解析协议）是一种协议，决定了链路层（第2层）地址，对于一个给定的网络层（第三层）地址。 ARP协议在RFC826以太网地址解析协议定义。

ARP协议被设计成允许被用于任何链路层和网络层协议。然而在实际中它仅用于以太网（包括802.11无线）和IPv4，我们假定在整个文档中，这些协议。 IPv6使用NDP（邻居发现协议）来代替，这是一种不同的协议

ARP是一个不可路由的协议，因此只能在同一个以太网网络上的系统之间使用

arp-scan参数:

```
-f <s>从指定文件中读取主机名或地址
-l从网络接口配置生成地址
-i 各扫描之间的时间差
-r 每个主机扫描次数
-t <i>设置主机超时时间
-V显示程序版本并退出
-I<s>使用网络接口
-g不显示重复的数据
-D显示数据包往返时间
```

arp-scan常用命令:

`arp-scan --interface=接口名 --localnet`

> --interface=接口名：代表要扫描的接口
> --localnet使 arp-scan：所有可能扫描的网络IP地址连接到这个接口上，通过接口的IP地址和网络掩码定义。你可以省略 - interface 选项，在这种情况下，arp-scan会搜索系统已配置了的接口列表中编号最小的（不包括环回）

`arp-scan --interface eth0 192.168.199.0/24`