Atk6-inverse_lookup6

"Atk6-inverse_lookup6"由www.github.com/vanhauser-thc/thc-ipv6出版，源自Atk6-IPv6-Attact-Toolkit（IPv6攻击包）项目，与Atk6-detest-new-ip6同样是Atk6-IPv6-Attact-Toolkit项目中的一个分支。

相对于Atk6-detest-ip6来说，Atk6-inverse-lookup6更是真对于MAC方面的，这句话在Atk6-inverse_lookup6的帮助手册之中：

"执行反向地址查询，以获取分配给MAC地址的IPv6地址。[^只有少数系统支持此功能]"

"Performs an inverse address query,to get the IPv6 addresses that are assigned to a MAC address. Note the only few system support this yet

——by van HHauser

1.帮助文档

atk6-inverse_lookup6 v3.6 (c) 2019 by van Hauser / THC vh@thc.org www.github.com/vanhauser-thc/thc-ipv6/vh@thc.org

语法:atk6-inverse_lookup6接口mac地址

执行反向地址查询，以获得所分配的IPv6地址
到MAC地址。请注意，目前只有少数系统支持此功能。

atk6-inverse_lookup6 v3.6 (c) 2019 by van Hauser / THC vh@thc.org www.github.com/vanhauser-thc/thc-ipv6

Syntax: atk6-inverse_lookup6 interface mac-address

Performs an inverse address query, to get the IPv6 addresses that are assigned
to a MAC address. Note that only few systems support this yet.

二，命令实例

Atk6-inverse_lookup6 vmnet8 00:0c:29:ec:86:13

向目标发送反向数据包

> *"在真实的环境中，我们是不知道对方MAC地址的，更不知道对方的IP地址。所以我们与要与Arping和Fping在配合Atk6_inverse_lookup6进行使用"*

Fing

Fping本次主要使用“-g参数”进行扫描整个网段的目标IP，通俗点来说就是对整个网段进行ping，发送数据包，如果有主机回应数据包则证明该主机活着，则在终端打印显示“0.0.0.0 is alive（0.0.0.0 还活着）”的亲切提醒

最后我们可得知目标的IP地址为 192.168.11.136

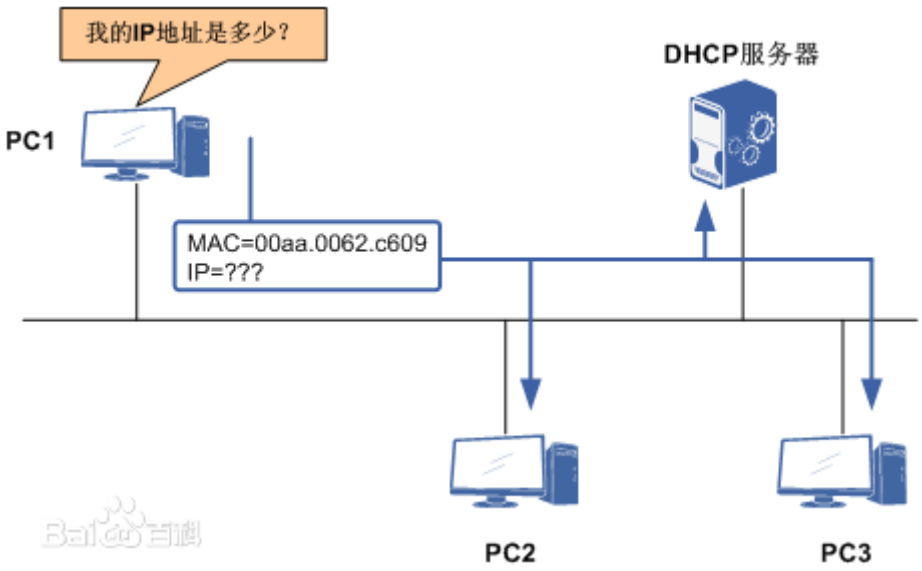
```
#fping -g 192.168.11.1/24
192.168.11.1 is alive
192.168.11.136 is alive
```

Arping

Arping主要获取对方的MAC地址，使用参数为“-r”，便可得知对方MAC地址为“00:0c:29:ec:86:13”

```
#arping -r 192.168.11.136
00:0c:29:ec:86:13
00:0c:29:ec:86:13
```

反向地址转换协议（RARP，Reverse Address Resolution Protocol）



逆地址解析协议（RARP，Reverse Address Resolution Protocol）

1.产生原因

逆地址解析协议主要这对与当一个设备只知道自己的物理地址（MAC），但不知道自身IP地址的情况下，就需使用逆地址解析协议。

就如我们目前所使用的Atk6-inverse_lookup6来说，Atk6-inverse_lookup6需要发送反向数据地址并希望对方可以返回其对应的地址。

2.工作原理

发送一个本地的RAPR广播，在广播之中，声称自己的MAC地址，并且让收到此请求的RARP服务器分配给自己一个IP地址。

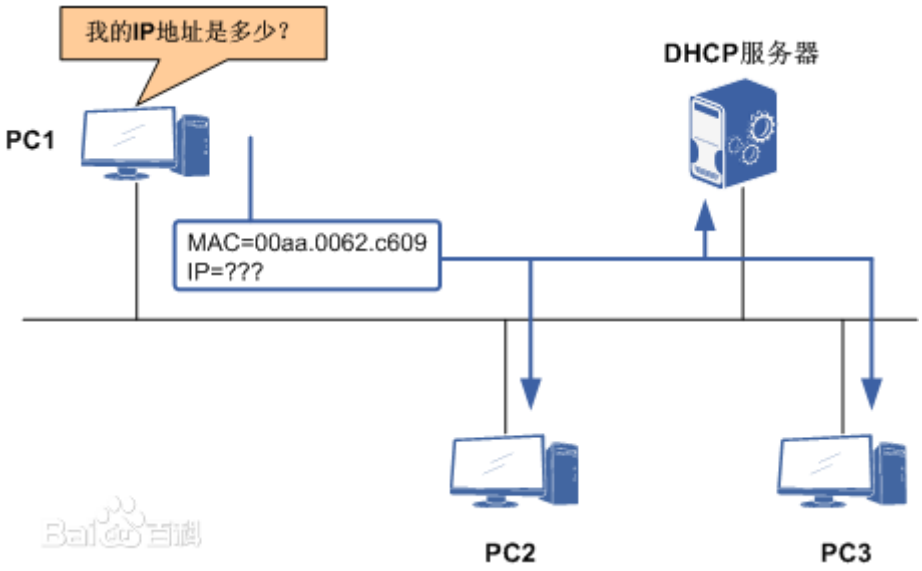
如果RARP服务器收到此请求后，检查其RARP列表，查找该MAC地址对应路由

如果存在，RARP服务器就会给源主机发送一个相应数据包并将IP地址提供给对方使用

如果不存在，RARP服务器不会做任何相应

> 如果已经拥有的，RARP服务器也不会做响应

3.工作过程



PC1从网卡中读取MAC地址，在网络中发放一个RARP广播请求数据包，请求RARP服务器回复该PC的IP地址

RARP服务器收到了RARP请求数据包，为其分配IP地址，并将RARP数据发送给PC1

PC1收到了其RARP发送的响应包即可完成此操作，并可以使用RARP响应的数据包中的IP地址进行通讯

参考文献：

> [反向地址转换协议] baike.baidu.com/item/反向地址转换协议/2991811#1