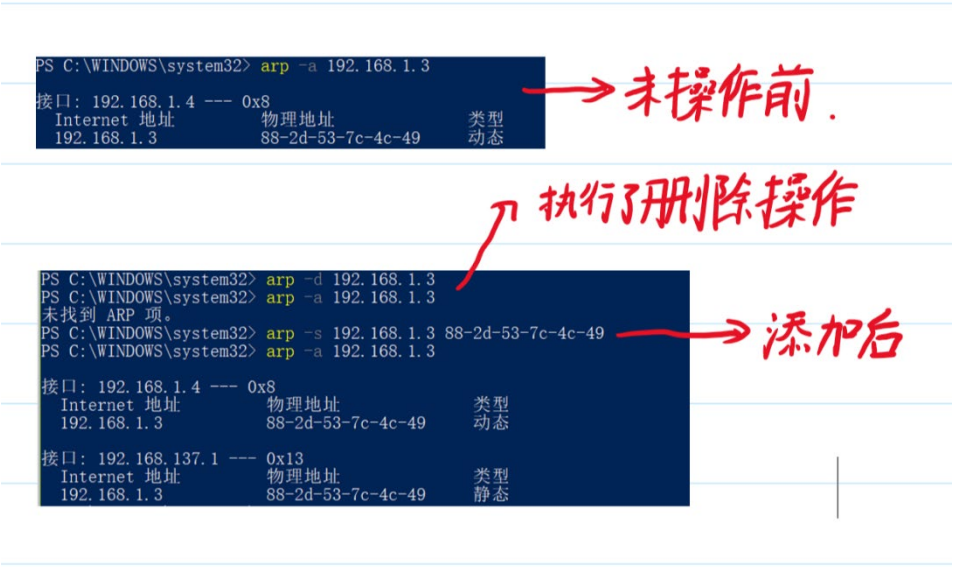
关于 ARP 指令的答疑

谢瑞桃

同学提问：老师，不好意思打扰了！我在使用 ARP 这个指令的时候遇到了一点问题。我删除 192.168.1.3 后，再次添加之后，出现了两个条目，而未操作前只有一个，不太清楚是怎么回事？见下图：



答疑：

1. arp -a 指令显示的是所有接口的 ARP 表。

2. arp -s 指令添加条目的时候是向哪个接口的 ARP 表添加呢？如果没有指定接口，那就选本机接口列表里的第一个。 那么你执行的那条添加指令加给谁了呢？那就是你 arp -a 列出的第一个接口。

3. 为什么删除之前有只有一个接口有那个 ARP 表项，但删除完以后有了两个呢？其中有一个一定不是你手工添加的，而是网络恰好在这个事件产生的。

理解这一点，需要 ARP 协议的知识。局域网中的通信寻址用的是 mac 地址。那么，当发送方要发数据给接收方，前者就需要后者的 mac 地址。怎么才能知道呢？通过 ARP 协议去发广播问，就像拿个大喇叭喊接收方 IP 地址的 MAC 地址是多少啊？因为是局域网里喊，如果对方在局域网里，就一定听得见，从而回复它。这就是 ARP 协议的用途，这是时时刻刻都在网络里发生的。

理解了上面这一点，就能解释你的问题了，你手动加了一个表项，另一个接口的表项是怎么来的呢？那应该就是在这段事件那个接口碰巧要跟你添加表项里的那个IP 地址的主机发生了通信，前者问出来的。有办法验证这一点，用 wireshark 抓包就能看到 ARP 协议的分组。

4. 你还可以做这样的实验，你把网关 IP 地址对应的表项删除。然后你用 arp -a 指令去查，会发现没多久那个表项自己就又出现了。