巧论ARP攻击防制方法之虚虚实实 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/251/2021_2022__E5_B7_A7_E8_AE_BAARP_E6_c101_251088.htm ARP欺骗/攻击反复袭击，是近来网络行业普遍了解的现象，随着ARP攻击的不断升级，不同的解决方案在市场上流传。但是笔者最近发现，有一些方案，从短期看来似乎有效，实际上对于真正的ARP攻击发挥不了作用，也降低局域网工作效率。Qno侠诺的技术服务人员接到很多用户反应说有些ARP防制方法很容易操作和实施，但经过实际深入了解后，发现长期效果都不大。 对于ARP攻击防制，Qno侠诺技术服务人员的建议，最好的方法是先踏踏实实把基本防制工作做好，才是根本解决的方法。由于市场上的解决方式众多，我们无法一一加以说明优劣，因此本文解释了ARP攻击防制的基本思想。我们认为读者如果能了解这个基本思想，就能自行判断何种防制方式有效，也能了解为何双向绑定是一个较全面又持久的解决方式。一、不坚定的ARP协议 一般计算机中的原始的ARP协议，很像一个思想不坚定，容易被其它人影响的人，ARP欺骗/攻击就是利用这个特性，误导计算机作出错误的行为。ARP攻击的原理，互联网上很容易找到，这里不再覆述。原始的ARP协议运作，会附在局域网接收的广播包或是ARP询问包，无条件覆盖本机缓存中的ARP/MAC对照表。这个特性好比一个意志不坚定的人，听了每一个人和他说话都信以为真，并立刻以最新听到的信息作决定。 就像一个没有计划的快递员，想要送信给"张三"，只在马路上问"张三住那儿？"，并投递给最近和他说"我就是！"或"张三住那间！"，来决定如何投递一

样。在一个人人诚实的地方，快递员的工作还是能切实地进行；但若是旁人看快递物品值钱，想要欺骗取得的话，快递员这种工作方式就会带来混乱了。 我们再回来看ARP攻击和这个意志不坚定快递员的关系。常见ARP攻击对象有两种，一是网络网关，也就是路由器，二是局域网上的计算机，也就是一般用户。攻击网络网关就好比发送错误的地址信息给快递员，让快递员整个工作大乱，所有信件无法正常送达；而攻击一般计算机就是直接和一般人谎称自己就是快递员，让一般用户把需要传送物品传送给发动攻击的计算机。 由于一般的计算机及路由器的ARP协议的意志都不坚定，因此只要有恶意计算机在局域网持续发出错误的ARP讯息，就会让计算机及路由器信以为真，作出错误的传送网络包动作。一般的ARP就是以这样的方式，造成网络运作不正常，达到盗取用户密码或破坏网络运作的目的。针对ARP攻击的防制，常见的方法，可以分为以下三种作法： 1、利用ARP echo传送正确的ARP讯息：通过频繁地提醒正确的ARP对照表，来达到防制的效果。 2、利用绑定方式，固定ARP对照表不受外来影响：通过固定正确的ARP对照表，来达到防制的效果。 3、舍弃ARP协议，采用其它寻址协议：不采用ARP作为传送的机制，而另行使用其它协议例如PPPoE方式传送。 以上三种方法中，前两种方法较为常见，第三种方法由于变动较大，适用于技术能力较佳的应用。下面针对前两种方法加以说明。 二、PK 赛之"ARP echo" ARP echo是最早开发出来的ARP攻击解决方案，但随着ARP攻击的发展，渐渐失去它的效果。现在，这个方法不但面对攻击没有防制效果，还会降低局域网运作的效能，但是很多用户仍然以这个方法来进行防制。

以前面介绍的思想不坚定的快递员的例子来说，ARP echo的作法，等于是时时用电话提醒快递员正确的发送对象及地址，减低他被邻近的各种信息干扰的情况。 但是这种作法，明显有几个问题：第一，即使时时提醒，但由于快递员意志不坚定，仍会有部份的信件因为要发出时刚好收到错误的信息，以错误的方式送出去；这种情况如果是错误的信息频率特高，例如有一个人时时在快递员身边连续提供信息，即使打电话提醒也立刻被覆盖，效果就不好；第二，由于必须时时提醒，而且为了保证提醒的效果好，还要加大提醒的间隔时间，以防止被覆盖，就好比快递员一直忙于接听总部打来的电话，根本就没有时间可以发送信件，耽误了正事；第三，还要专门指派一位人时时打电话给快递员提醒，等于要多派一个人手负责，而且持续地提醒，这个人的工作也很繁重。以ARP echo方式对应ARP攻击，也会发生相似的情况。第一，面对高频率的新式ARP攻击，ARP echo发挥不了效果，掉线断网的情况仍旧会发生。ARP echo的方式防制的对早期以盗宝为目的的攻击软件有效果，但碰到最近以攻击为手段的攻击软件则公认是没有效果的。第二，ARP echo手段必须在局域网上持续发出广播网络包，占用局域网带宽，使得局域网工作的能力降低，整个局域网的计算机及交换机时时都在处理ARP echo广播包，还没受到攻击局域网就开始卡了。第三，必须在局域网有一台负责负责发ARP echo广播包的设备，不管是路由器、服务器或是计算机，由于发包是以一秒数以百计的方式来发送，对该设备都是很大的负担。 