巧论 ARP 攻击防制方法之虚虚实实

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。

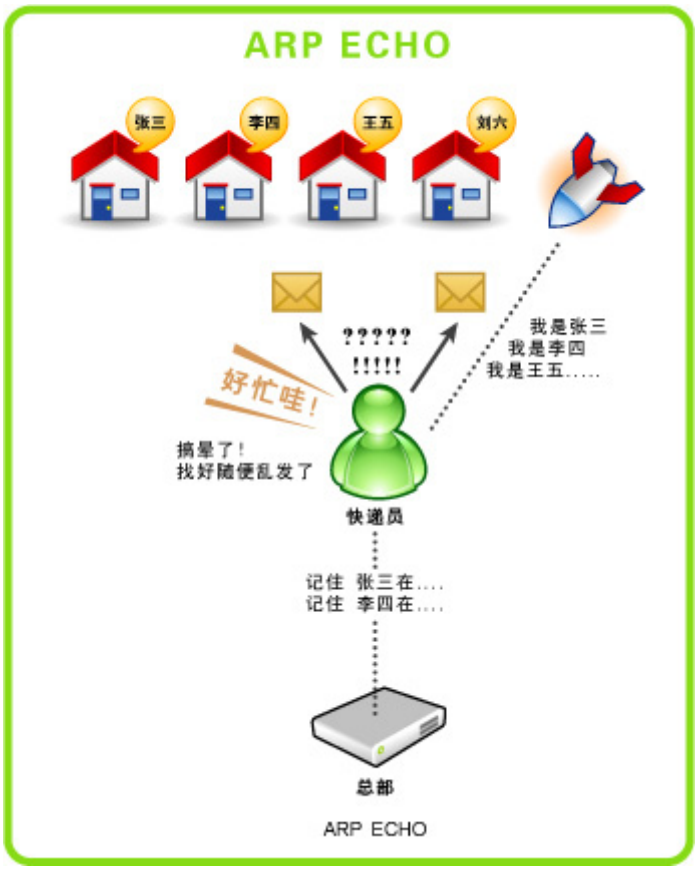
- **PK 赛之“ARP echo”**

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。



图一：ARP 攻击防制 方法之“ARP echo”图示说明

常见的 ARP echo 处理手法有两种，一种是由路由器持续发送，另一则是在计算机或服务器安装软件发送。路由器持续发送的缺点是路由器原本的工作就很忙，因此无法发送高频率的广播包，被覆盖掉的机会很大，因此面对新型的 ARP 攻击防制效果小。因此，有些解决方法，就是拿 ARP 攻击的软件来用，只是持续发出正确的网关、服务器对照表，安装在服务器或是计算机上，由于服务器或是计算机运算能力较强，可以同一时间内发出更多广播包，效果较大，但是这种作法一则大幅影响局域网工作，因为整个局域网都被广播包占据，另则攻击软件通常会设定更高频率的广播包，误导局域网计算机，效果仍然有限。

此外，ARP echo 一般是发送网关及私服的对照信息，对于防止局域网计算机被骗有效果，对于路由器没有效果，仍需作绑定的动作才可。

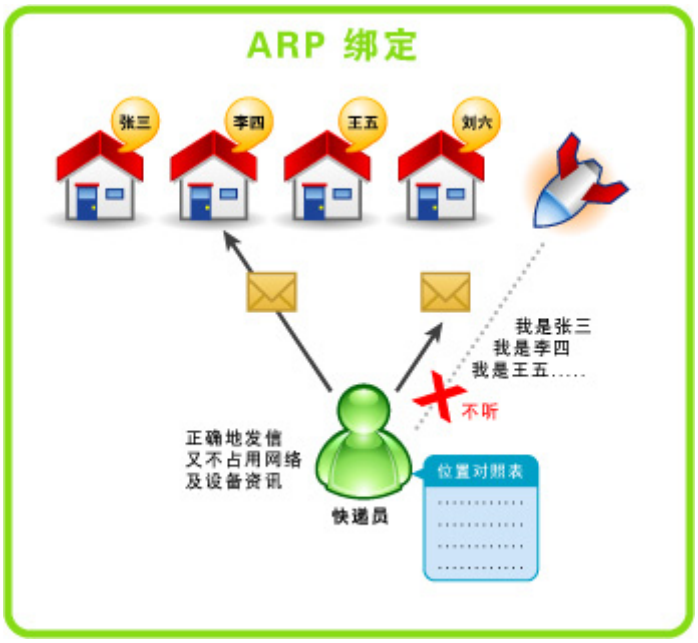
- **PK 赛之“ARP 绑定”**

ARP echo 的作法是不断提醒计算机正确的 ARP 对照表，ARP 绑定则是针对 ARP 协议“思

想不坚定“的基本问题来加以解决。Qno 侠诺技术服务人员认为，ARP 绑定的作法，等于是从基本上给这个快递员培训，让他把正确的人名及地址记下来，再也不受其它人的信息干扰。由于快递员脑中记住了这个对照表，因此完全不会受到有心人士的干扰，能有效地完成工作。在这种情况下，无论如何都可以防止因受到攻击而掉线的情况发生。

但是 ARP 绑定并不是万灵药，还需要作的好才有完全的效果。第一，即使这个快递员思想正确，不受影响，但是攻击者的网络包还是会小幅影响局域网部份运作，网管必须通过网络监控或扫瞄的方法，找出攻击者加以去除；第二，必须作双向绑定才有完全的效果，只作路由器端绑定效果有限，一般计算机仍会被欺骗，而发生掉包或掉线的情况。

双向绑定的解决方法，最为网管不喜欢的就是必须一台一台加以绑定，增加工作量。但是从以上的说明可知道，只有双向绑定才能有效果地解决 ARP 攻击的问题，而不会发生防制效果不佳、局域网效率受影响、影响路由器效能或影响服务器效能的缺点。也就是说双向绑定是个硬工夫，可以较全面性地解决现在及未来 ARP 攻击的问题，网管为了一时的省事，而采取片面的 ARP echo 解决方式，未来还是要回来解决这个问题。



图二：ARP 攻击防制 方法之侠诺“ARP 双向绑定”图示说明

另外，对于有自动通过局域网安装软件的网络，例如网吧的收费系统、无盘系统，都可以透过自动的批次档，自动在开机时完成绑定的工作，网管只要撰写一个统一的批次文件程序即可，不必一一配置。这些信息可以很容易地在互联网上通过搜索找到或者是向 Qno 侠

诺的技术服务人员索取即可。

二、现阶段较佳解决方案——双向绑定

以上以思想不坚定的快递员情况，说明了常见的 ARP 攻击防制方法。ARP 攻击利用的就是 ARP 协议的意志不坚，只有以培训的方式让 ARP 协议的意志坚定，明白正确的工作方法，才能从根本解决问题。只是依赖频繁的提醒快递员正确的作事方法，但是没有能从快递员意志不坚的特点着手，就好像只管不教，最终大家都很累，但是效果仍有限。

Qno 侠诺的技术服务人员建议，面对这种新兴攻击，取巧用省事的方式准备，最后的结果可能是费事又不管用，必须重新来过。ARP 双向绑定虽然对网管带来一定的工作量，但是其效果确是从根本上有效，而且网管也可参考自动批次档的作法，加快配置自动化的进行，更有效地对抗 ARP 攻击。