自身的 ARP 缓存表，查看里面是否有 192.168.0.4 这台电脑的 MAC 地址，如果有，就将 MAC-D 封装在数据包的外面，直接发送出去即可。如果没有，S 电脑便向全网络发送一个这样的 ARP 广播包:S 的 IP 是 192.168.0.3，硬件地址是 MAC-S，要求返回 IP 地址为 192.168.0.4 的主机的硬件地址。而 D 电脑接受到该广播，经核实 IP 地址，则将自身的 IP 地址和 MAC-D 地址返回到 S 电脑。现在 S 电脑可以在要发送的数据包上贴上目的地址 MAC-D 发送出去，同时它还会动态更新自身的 ARP 缓存表，将 192.168.0.4-MAC-D 这一条记录添加进去，这样，等 S 电脑下次再给 D 电脑发送数据的时候，发送 ARP 广播包进行查询了。这就是正常情况下的数据包发送过程。

但是，上述数据发送机制有一个致命的缺陷，即它是建立在对局域网中电脑全部信任的基础上的，也就是说它的假设前提是:无论局域网中哪台电脑，其发送的 ARP 数据包都是正确的。比如在上述数据发送中，当 S 电脑向全网询问后，D 电脑也回应了自己的正确 MAC 地址。但是当此时，A 电脑却返回了 D 电脑的 IP 地址和自己的硬件地址。由于 A 电脑不停地发送这样的应答数据包，则会导致 S 电脑又重新动态更新自身的 ARP 缓存表，这回记录成:192.168.0.4 与 MAC-A 对应，我们把这步叫做 ARP 缓存表中毒。这样，就导致以后凡是 S 电脑要发送给 D 电脑，都将会发送给 A 主机。也就是说，A 电脑就劫持了由 S 电脑发送给 D 电脑的数据。这就是 ARP 欺骗的过程。

如果 A 电脑不冒充 D 电脑，而是冒充网关，那后果会更加严重。一个局域网中的电脑要连接外网，都要经过局域网中的网关进行转发。在局域网中，网关的 IP 地址假如为 192.168.0.1。如果 A 电脑向全网不停的发送 IP 地址是 192.168.0.1，硬件地址是 MAC-A 的 ARP 欺骗广播，局域网中的其它电脑都会更新自身的 ARP 缓存表，将 A 电脑当成网关，这样，当它们发送数据给网关，结果都会发送到 MAC-A 这台电脑中。这样，A 电脑就将会监听整个局域网发送给互联网的数据包。

4 结 语

ARP 欺骗是目前网络管理，特别是校园网管理中最让人头疼的攻击，它的攻击技术含量低，随便一个人都可以通过攻击软件来完成 ARP 欺骗攻击。同时防范 ARP 欺骗也没有什么特别有效的方法，目前只能通过被动的亡羊补牢形式的措施了。无论是攻和防，首要的就是找出每种攻击的“症结”之所在。只有这样才能找到行之有效的解决方案。当然最根本的办法在客户端自身的防范上，如及时下载安装系统补丁、所装杀毒软件及时升级，安装 ARP 专杀与防范软件等。

法兰克福产业用展开幕在即，航天用高技术纺织品受关注

全球产业用纺织品领域知名的 Techtextil 法兰克福国际产业用纺织品及非织造布展览会，将于 5 月 9 日～5 月 12 日在德国举行。今年展会除了全产业链展示产业用高新技术的最新成果和应用外，多项创新技术含金量更高，活动内容也更丰富，覆盖面更广，吸引了行业高度关注。其中，展会与欧洲航天局和德国宇航中心联手打造的“太空生活”项目，将成为本届展会的最大亮点。

据法兰克福展览有限公司纺织品及纺织技术展副总裁 Olaf Schmidt 介绍，今年的 Techtextil 展不断拓展新的领域，参展总体规模已超过上届。今年，主办方在产业用纺织品的一大主要应用领域与新的合作伙伴欧洲航天局（ESA）和德国宇航中心（DLR）联手推出“太空生活”项目，将充分展示产业用纺织品在航空工业的大量应用案例，全方位展示产业用高新技术在相关领域的应用。

该专区的展品范围包括太空领域的高科技纺织品及纺织品加工技术的发端和应用。虚拟现实体验是互动专区的一大亮点。观众可以在此体验通向火星的虚拟太空旅程，探索产业用纺织品及其加工技术如何帮助人类成功在太空建立社区。在相关主题内容展区，多家参展商将集中展示与太空旅行有关的纺织产品及加工技术。

Texprocess 法兰克福国际纺织品及柔性材料缝制加工展览会也将于 5 月 9~5 月 12 日在法兰克福展览中心同期同地举行，为业界展示整理和数码印花等纺织品加工全过程的最新技术、产品和应用。

摘自《中国纺织报》