文章编号：1006-4354 (2008) 05-0046-02

局域网 ARP 病毒及防范

陈百川，周 军

(陕西省气象局后勤服务中心，西安 710014)

中图分类号：P409 **文献标识码**：B

陕西省气象局两大院局域网络开通后，各网段都不同程度出现了上网速度有时很慢、常掉线甚至上不了网的情况，经过检查发现，大多数是由于网段内存在 ARP 病毒攻击所至。

1 ARP 协议

ARP (Address Resolution Protocol) 为地址解析协议。是 TCP/IP 协议栈中的低层协议，主要作用是将 IP 地址解析成对应的 MAC 地址。在局域网中，IP 数据包在局域网内部传输并不是靠 IP 地址而是靠 MAC 地址来识别目标的，所以 IP 地址与 MAC 地址逐一对应，ARP 协议就是用来确定这种对应关系的。

2 ARP 攻击

通过对 ARP 协议的认识，了解局域网内数据包传输是依靠 MAC 地址，IP 地址与 MAC 地址对应关系依靠 ARP 映射表，每台主机包括路由器都有一个 ARP 缓存表，在无 ARP 欺骗的情况下，主机 ARP 缓存表能够保证数据传输的准确性，但 ARP 缓存表的更新存在一个不完善的地方——易信任性，即对发来的 ARP 数据包的正确与否不做审查，当主机接收到刻意编制的，将 IP 地址指向错误的 MAC 地址的 ARP 数据包，主机也会不加审查将其加入 ARP 缓存表，这样，当主机下次访问此 IP 时，就根据这个虚假的记录，把数据发送到记录所对应的错误 MAC 地址，而真正使用这个 IP 的主机则收不到数据，这就是所谓的 ARP 欺骗原理。一个局域网网段内的主机要与外网通信，必须经过局域网与外网之间的节点—网关，由于存在主机必须与之通信的理由，将网关 IP 地址与错误的 MAC 地址对应，也就成为大部分 ARP 欺骗行为。

3 ARP 病毒的传输方式及危害

ARP 欺骗是一种攻击方式，所有的病毒都可以采用这种方式，主要通过网页下载传播、网络共享传播、移动存储介质传播和文件感染等。虽然 ARP 病毒的目的不同，但都会影响局域网网段内的所有主机和网关，让所有上网的流量必须经过 ARP 攻击者控制的主机或被转发它处，用户原来直接通过网关上网转由被控主机和转发上网或者根本上不了网，由于转发不会非常流畅，导致用户上网速度变慢，或上网时断时续。其危险之处在于其一，攻击者可以借此控制用户主机的数据流向，使得用户主机访问网关失败，导致用户无法与外网通信；其二，让用户主机发送的数据传输到不该传输的地方，MAC 地址所对应的主机，将接收到原应发到网关的数据，如收到数据主机直接将数据丢弃，后果是被欺骗主机得不到回应，不能正常上网，如果收到数据主机以“伪网关”充当“真网关”的替代者，成为数据中继站，则上网主机就有可能暴露敏感信息（如游戏账号和密码、QQ 号和密码、网银帐号和密码）。

4 ARP 病毒的防范

ARP 欺骗只是 ARP 病毒的一种行为和表现，病毒性质不同，并不是一种病毒变种的集合，避免电脑感染 ARP 病毒和预防其它病毒一样，应从修补软件漏洞，加强安全防护，养成良好的上网习惯着手。还可从局域网每个网段的路由器着手，对 IP 地址和 MAC 地址进行编制绑定，对

收稿日期：2008-03-31

作者简介：陈百川 (1959-)，男，广东大埔人，工程师，从事电气设备及网络维护管理。

文章编号：1006-4354（2008）05-0047-03

GTS1 型数字式探空仪施放前的准备工作

王雯燕，唐文哲

（西安市气象局，西安 710016）

中图分类号：P414 文献标识码：B

GTS1 型数字式探空仪是一次性使用的高空气象仪器，具有探测精度高、采样速度快、抗干扰能力强等特点，实现了数字化、模块化，整体性能好。GTS1 型数字式探空仪使用前不用进行灵敏度检查和基点检查，基测方便，不受外界天气的影响，检测数据稳定可靠。探空仪载频采用了多重调制技术，提高了探空发送传递数据的可靠性和抗同频干扰的能力，但是 GTS1 型数字式探空仪施放前的准备工作要求较高，稍有失误就会影响本次探测资料的完整性或造成重放球。

1 湿度传感器（湿敏元件）

（1）湿敏元件采用 XGH-02 型高分子弹性材料和按一定比例混合的吸湿材料，含有 TX-100、三梨醇（张力辅助材料）、炭黑等成分的有机玻璃基片组成。炭黑等材料高湿时膨胀电阻值大，低湿时收缩电阻值小。湿度传感器阻值具有二元特性，与测量环境的温度、湿度都有关系。湿敏元件使用时互换性能好，出厂每瓶 10 个，同一批次 2 000 个左右都可互换。

（2）湿敏元件是一次性使用元件，出厂时置于密封的管内，取出后不能直接使用，在施放前必须老化并基测合格后方可施放。高湿老化在放球前 1 h 进行，时间要求达 1 min 以上，实践证明升湿阻值越大越好，达到 800 kΩ 左右元件合格率较高。注意：湿敏元件高湿老化时，如发现瓶底有结晶体盐时，按配制方法向容器内加入适量蒸馏水。湿敏元件在高湿瓶中如发现升湿几分钟还达不到 300 kΩ 以上时，应检查湿敏元件插入专用插座上是否有白色的硫酸钾晶体，如有可用小纸片插入专用插座的电极片中擦拭，擦净后重复老化即可。

（3）湿敏元件的阻值随时间变化也有漂移，因此在使用过程中采用比阻值来测量相对湿度。用某一相对湿度阻值做为参考，其它湿度的阻值与其相比。瓶内用于做比较的干燥剂为颗粒状硅胶，又叫变色硅胶，其相对湿度在 3%或以下，利用硅干燥剂提供的湿度环境进行基测前的老化降湿过程。干燥剂随着时间的推移，湿度平衡交换次数的增加其吸湿能力逐渐降低。为此要注意干燥剂是否失效，正常状态为蓝色，吸收水分渐渐变为紫红色，以颜色变浅作为判断的依据。建议湿度大的台站一星期更换二次，湿度小于 30%的台站可半个月更换一次，剂量以不触及湿敏元件为准，通常保持瓶内的湿度在 0%～3%之间，才能保证稳定后读的基值 R_0 正确无误。

（4）将 R_0、T_0 数据输入计算机，数据不要输反。每箱仪器的湿敏元件与温、压传感器不一定能刚好配套使用，数据输入计算机时要仔细核对

收稿日期：2008-05-21

作者简介：王雯燕（1972-），女，陕西大荔人，工程师，从事高空气象观测。

每台上网主机 IP 与 MAC 地址的绑定，但遇到设备更新、升级等情况，由于主机的 MAC 地址发生变更，就需对路由器及主机从新作绑定工作。在无绑定的情况下，每台上网主机安装 ARP 防火墙是比较可行，另外做为网络管理者，发现网络内有 ARP 攻击者，应及时锁定 IP 及 MAC 地址，关闭其上网端口，对病毒进行查杀处理，保障网络系统的正常运行。