 一般ARP攻击的对治方法： 现在最常用的基本对治方法是“ ARP双向绑定 ”。由于ARP攻击往往不是病毒造成的，而是合法运行的程序(外挂、网页)造成的，所杀毒软件多数时候束手无策。 所谓“ 双向绑定 ”，就是再路由器上绑定ARP表的同时，在每台电脑上也绑定一些常用的ARP表项。“ ARP双向绑定 ”能够防御轻微的、手段不高明的ARP攻击。ARP攻击程序如果没有试图去更改绑定的ARP表项，那么ARP攻击就不会成功.如果攻击手段不剧烈，也欺骗不了路由器，这样我们就能够防住50%ARP攻击。 但是现在ARP攻击的程序往往都是合法运行的，所以能够合法的更改电脑的ARP表项。在现在ARP双向绑定流行起来之后，攻击程序的作者也提高了攻击手段，攻击的方法更综合，另外攻击非常频密，仅仅进行双向绑定已经不能够应付凶狠的ARP攻击了，仍然很容易出现掉线。 于是我们在路由器中加入了“ ARP攻击主动防御 ”的功能。这个功能是在路由器ARP绑定的基础上实现的，原理是：当网内受到错误的ARP广播包攻击时，路由器立即广播正确的ARP包去修正和消除攻击包的影响。这样我们就解决了掉线的问题，但是在最凶悍的ARP攻击发生时，仍然发生了问题----当ARP攻击很频密的时候，就需要路由器发送更频密的正确包去消除影响。虽然不掉线了，但是却出现了上网“ 卡 ”的问题。 所以，我们认为，依靠路由器实现“ ARP攻击主动防御 ”，也只能够解决80%的问题。 为了彻底消除ARP攻

击，我们在此基础上有增加了“ ARP攻击源攻击跟踪 ”的功能。对于剩下的强悍的ARP攻击，我采用“ 日志 ”功能，提供信息方便用户跟踪攻击源，这样用户通过临时切断攻击电脑或者封杀发出攻击的程序，能够解决问题。 彻底解决ARP攻击 事实上，由于路由器是整个局域网的出口，而ARP攻击是以整个局域网为目标，当ARP攻击包已经达到路由器的时候，影响已经照成。所以由路由器来承担防御ARP攻击的任务只是权宜之计，并不能很好的解决问题。 我们要真正消除ARP攻击的隐患，安枕无忧，必须转而对“ 局域网核心 ”——交换机下手。由于任何ARP包，都必须经由交换机转发，才能达到被攻击目标，只要交换机据收非法的ARP包，哪么ARP攻击就不能造成任何影响。 我们提出一个真正严密的防止ARP攻击的方案，就是在每台接入交换机上面实现ARP绑定，并且过滤掉所有非法的ARP包。这样可以让ARP攻击足不能出户，在局域网内完全消除了ARP攻击。 因为需要每台交换机都具有ARP绑定和相关的安全功能，这样的方案无疑价格是昂贵的，所以我们提供了一个折衷方案。 解决方案 我们只是中心采用能够大量绑定ARP和进行ARP攻击防御的交换机——Netcore 7324NSW，这款交换机能够做到ARP绑定条目可以达到1000条，因此基本上可以对整网的ARP进行绑定，同时能杜绝任何非法ARP包在主交换机进行传播。 这样如果在强力的ARP攻击下，我们观察到的现象是：ARP攻击只能影响到同一个分支交换机上的电脑，这样可能被攻击到的范围就大大缩小了。当攻击发生时，不可能造成整个网络的问题。 在此基础上，我们再补充“ 日志 ”功能和“ ARP主动防御 ”功能，ARP攻击也可以被完美的解决。 ARP攻击最

新动态 最近一段时间，各网吧发现的ARP攻击已经升级，又一波ARP攻击的高潮来临。 这次ARP攻击发现的特征有： 1、速度快、效率高，大概在10-20秒的时间内，能够造成300台规模的电脑掉线。 2、 不易发现。在攻击完成后，立即停止攻击并更正ARP信息。如果网内没有日志功能，再去通过ARP命令观察，已经很难发现攻击痕迹。 3、 能够破解最新的XP和2000的ARP补丁，微软提供的补丁很明显在这次攻击很脆弱，没有作用。 4、 介质变化，这次攻击的来源来自私服程序本身(不是外挂)和P2P程序。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com