 最近在论坛上经常看到关于ARP病毒的问题，于是在Google上搜索ARP关键字，结果出来很多关于这类问题的讨论。呵呵，俺的求知欲很强，想再学习ARP下相关知识，所以对目前网络中常见的ARP问题进行了一个总结。 1. ARP概念 咱们谈ARP之前，还是先要知道ARP的概念和工作原理，理解了原理知识，才能更好去面对和分析处理问题。 1.1 ARP概念知识 ARP，全称Address Resolution Protocol，中文名为地址解析协议，它工作在数据链路层，在本层和硬件接口联系，同时对上层提供服务。 IP数据包常通过以太网发送，以太网设备并不识别32位IP地址，它们是以48位以太网地址传输以太网数据包。因此，必须把IP目的地址转换成以太网目的地址。在以太网中，一个主机要和另一个主机进行直接通信，必须要知道目标主机的MAC地址。但这个目标MAC地址是如何获得的呢？它就是通过地址解析协议获得的。ARP协议用于将网络中的IP地址解析为的硬件地址（MAC地址），以保证通信的顺利进行。 1.2 ARP工作原理 首先，每台主机都会在自己的ARP缓冲区中建立一个 ARP列表，以表示IP地址和MAC地址的对应关系。当源主机需要将一个数据包要发送到目的主机时，会首先检查自己 ARP列表中是否存在该 IP地址对应的MAC地址，如果有就直接将数据包发送到这个MAC地址；如果没有，就向本地网段发起一个ARP请求的广播包，查询此目的主机对应的MAC地址。此ARP请求数据包里包括源主机的IP地址、硬件

地址、以及目的主机的IP地址。网络中所有的主机收到这个ARP请求后，会检查数据包中的目的IP是否和自己的IP地址一致。如果不相同就忽略此数据包；如果相同，该主机首先将发送端的MAC地址和IP地址添加到自己的ARP列表中，如果ARP 表中已经存在该IP的信息，则将其覆盖，然后给源主机发送一个 ARP响应数据包，告诉对方自己是它需要查找的MAC地址；源主机收到这个ARP响应数据包后，将得到的目的主机的IP地址和MAC地址添加到自己的 ARP列表中，并利用此信息开始数据的传输。如果源主机一直没有收到ARP响应数据包，表示ARP查询失败。 例如： A的地址为：IP：192.168.10.1 MAC： AA-AA-AA-AA-AA-AA B的地址为：IP：192.168.10.2 MAC： BB-BB-BB-BB-BB-BB 根据上面的所讲的原理，我们简单说明这个过程：A要和B通讯，A就需要知道B的以太网地址，于是A发送一个ARP请求广播（谁是192.168.10.2，请告诉192.168.10.1），当B收到该广播，就检查自己，结果发现和自己的一致，然后就向A发送一个ARP单播应答（192.168.10.2 在BB-BB-BB-BB-BB-BB）。 1.3 ARP通讯模式 通讯模式（Pattern Analysis）：在网络分析中，通讯模式的分析是很重要的，不同的协议和不同的应用都会有不同的通讯模式。更有些时候，相同的协议在不同的企业应用中也会出现不同的通讯模式。ARP在正常情况下的通讯模式应该是：请求 -> 应答 -> 请求 -> 应答，也就是应该一问一答。 2. 常见ARP攻击类型 个人认为常见的ARP攻击为两种类型：ARP扫描和ARP欺骗。 2.1 ARP扫描（ARP请求风暴） 通讯模式（可能）： 请求 -> 请求 -> 请求 -> 请求 -> 请求 -> 请求 -> 应答 -> 请求 -> 请求 -> 请求…… 描述： 网络中出现大

量ARP请求广播包，几乎都是对网段内的所有主机进行扫描。大量的ARP请求广播可能会占用网络带宽资源；ARP扫描一般为ARP攻击的前奏。 出现原因（可能）：*病毒程序，侦听程序，扫描程序。*如果网络分析软件部署正确，可能是我们只镜像了交换机上的部分端口，所以大量ARP请求是来自与非镜像口连接的其它主机发出的。*如果部署不正确，这些ARP请求广播包是来自和交换机相连的其它主机。 2.2 ARP欺骗 ARP协议并不只在发送了ARP请求才接收ARP应答。当计算机接收到ARP应答数据包的时候，就会对本地的ARP缓存进行更新，将应答中的IP和MAC地址存储在ARP缓存中。所以在网络中，有人发送一个自己伪造的ARP应答，网络可能就会出现问题。这可能就是协议设计者当初没考虑到的！ 2.2.1 欺骗原理 假设一个网络环境中，网内有三台主机，分别为主机A、B、C.主机详细信息如下描述： A的地址为：IP：192.168.10.1 MAC： AA-AA-AA-AA-AA-AA B的地址为：IP：192.168.10.2 MAC： BB-BB-BB-BB-BB-BB C的地址为：IP：192.168.10.3 MAC： CC-CC-CC-CC-CC-CC 正常情况下A和C之间进行通讯，但是此时B向A发送一个自己伪造的ARP应答，而这个应答中的数据为发送方IP地址是192.168.10.3（C的IP地址），MAC地址是BB-BB-BB-BB-BB-BB（C的MAC地址本来应该是CC-CC-CC-CC-CC-CC，这里被伪造了）。当A接收到B伪造的ARP应答，就会更新本地的ARP缓存（A被欺骗了），这时B就伪装成C了。同时，B同样向C发送一个ARP应答，应答包中发送方IP地址四192.168.10.1（A的IP地址），MAC地址是BB-BB-BB-BB-BB- BB（A的MAC地址本来应该是AA-AA-AA-AA-AA-AA），当C收到B伪造的ARP应答

，也会更新本地ARP缓存（C也被欺骗了），这时B就伪装成了A.这样主机A和C都被主机B欺骗，A和C之间通讯的数据都经过了B.主机B完全可以知道他们之间说的什么：）。这就是典型的ARP欺骗过程。 注意：一般情况下，ARP欺骗的某一方应该是网关。 2.2.2 两种情况 ARP欺骗存在两种情况：一种是欺骗主机作为“ 中间人 ”，被欺骗主机的数据都经过它中转一次，这样欺骗主机可以窃取到被它欺骗的主机之间的通讯数据；另一种让被欺骗主机直接断网。 第一种：窃取数据（嗅探） 通讯模式： 应答 -> 应答 -> 应答 -> 应答 -> 应答 -> 请求 -> 应答 -> 应答 ->请求->应答…… 描述： 这种情况就属于我们上面所说的典型的ARP欺骗，欺骗主机向被欺骗主机发送大量伪造的ARP应答包进行欺骗，当通讯双方被欺骗成功后，自己作为了一个“ 中间人 ”的身份。此时被欺骗的主机双方还能正常通讯，只不过在通讯过程中被欺骗者“ 窃听 ”了。 出现原因（可能）：*木马病毒 *嗅探 *人为欺骗 第二种：导致断网 通讯模式： 应答 -> 应答 -> 应答 -> 应答 -> 应答 -> 应答 -> 请求… 描述： 这类情况就是在ARP欺骗过程中，欺骗者只欺骗了其中一方，如B欺骗了A，但是同时B没有对C进行欺骗，这样A实质上是在和B通讯，所以A就不能和C通讯了，另外一种情况还可能就是欺骗者伪造一个不存在地址进行欺骗。 对于伪造地址进行的欺骗，在排查上比较有难度，这里最好是借用TAP设备（呵呵，这个东东好像有点贵勒），分别捕获单向数据流进行分析！ 出现原因（可能）：* 木马病毒 *人为破坏 *一些网管软件的控制功能 3. 常用的防护方法 搜索网上，目前对于ARP攻击防护问题出现最多是绑定IP和MAC和使用ARP防护软件，也出现了具有ARP防护功

能的路由器。呵呵，我们来了解下这三种方法。 3.1 静态绑定 最常用的方法就是做IP和MAC静态绑定，在网内把主机和网关都做IP和MAC绑定。 欺骗是通过ARP的动态实时的规则欺骗内网机器，所以我们把ARP全部设置为静态可以解决对内网PC的欺骗，同时在网关也要进行IP和MAC的静态绑定，这样双向绑定才比较保险。 方法： 对每台主机进行IP和MAC地址静态绑定。 通过命令，arp -s可以实现“ arp s IP MAC地址 ”。 例如：“ arp s 192.168.10.1 AA-AA-AA-AA-AA-AA ”。 如果设置成功会在PC上面通过执行 arp -a 可以看到相关的提示 ： 一般不绑定，在动态的情况下： 说明：对于网络中有很多主机，500台，1000台……，如果我们这样每一台都去做静态绑定，工作量是非常大的……，这种静态绑定，在电脑每次重起后，都必须重新在绑定，虽然也可以做一个批处理文件，但是还是比较麻烦的！ 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