ARP地址解析协议介绍 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/490/2021_2022_ARP_E5_9C_B0_E5_9D_80_E8_c67_490693.htm ARP（AddressResolutionProtocol）地址解析协议用于将计算机的网络地址（IP地址32位）转化为物理地址（MAC地址48位）[RFC826].ARP协议是属于链路层的协议，在以太网中的数据帧从一个主机到达网内的另一台主机是根据48位的以太网地址（硬件地址）来确定接口的，而不是根据32位的IP地址。内核（如驱动）必须知道目的端的硬件地址才能发送数据。当然，点对点的连接是不需要ARP协议的。 ARP协议的数据结构： 以下是引用片段： typedefstructarphdr { unsignedshortarp_hrd./*硬件类型*/ unsignedshortarp_pro./*协议类型*/ unsignedchararp_hln./*硬件地址长度*/ unsignedchararp_pln./*协议地址长度*/ unsignedshortarp_op./*ARP操作类型*/ unsignedchararp_sha[6]./*发送者的硬件地址*/ unsignedlongarp_spa./*发送者的协议地址*/ unsignedchararp_tha[6]./*目标的硬件地址*/ unsignedlongarp_tpa./*目标的协议地址*/ }ARPHDR,*PARPHDR. 为了解释ARP协议的作用，就必须理解数据在网络上的传输过程。这里举一个简单的PING例子。假设我们的计算机IP地址是192.168.1.1，要执行这个命令：ping192.168.1.2.该命令会通过ICMP协议发送ICMP数据包。该过程需要经过下面的步骤： 1、应用程序构造数据包，该示例是产生ICMP包，被提交给内核（网络驱动程序）；2、

内核检查是否能够转化该IP地址为MAC地址，也就是在本地的ARP缓存中查看IP-MAC对应表；3、如果存在该IP-MAC对应关系，那么跳到步骤9；如果不存在该IP-MAC对应关系，那么接续下面的步骤；4、内核进行ARP广播，目的地的MAC地址是FF-FF-FF-FF-FF-FF，ARP命令类型为REQUEST（1），其中包含有自己的MAC地址；5、当192.168.1.2主机接收到该ARP请求后，就发送一个ARP的REPLY（2）命令，其中包含自己的MAC地址；6、本地获得192.168.1.2主机的IP-MAC地址对应关系，并保存到ARP缓存中；7、内核将把IP转化为MAC地址，然后封装在以太网头结构中，再把数据发送出去；使用arp-a命令就可以查看本地的ARP缓存内容，所以，执行一个本地的PING命令后，ARP缓存就会存在一个目的IP的记录了。当然，如果你的数据包是发送到不同网段的目的地，那么就一定存在一条网关的IP-MAC地址对应的记录。 知道了ARP协议的作用，就能够很清楚地知道，数据包的向外传输很依靠ARP协议，当然，也就是依赖ARP缓存。要知道，ARP协议的所有操作都是内核自动完成的，同其他的应用程序没有任何关系。同时需要注意的是，ARP协议只使用于本网络。 ARP协议的利用和相关原理介绍。 一、交换网络的嗅探 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。因此，在上面的假设网络中，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DD-DD-DD-DD-DD-DD（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，将本地的IP-MAC对应表更换为接收到的数据格式，由于这一切都是A的系统内核自动完成的，A可不知道被伪造了。 ARP欺骗的主要用途就是进行在交换网络中的嗅探。有关交换网络的嗅探不是本文的讨论内容。 二、IP地址冲突 我们知道，如果网络中存在相同IP地址的主机的时候，就会报告出IP地址冲突的警告。这是怎么产生的呢？ 比如某主机B规定IP地址为192.168.0.1，如果它处于开机状态，那么其他机器A更 改IP地址为192.168.0.1就会造成IP地址冲突。其原理就是：主机A在连接网络（或更改IP地址）的时候就会向网络发送ARP包广播自己的IP地址，也就是freearp.如果网络中存在相同IP地址的主机B，那么B就会通过ARP来reply该地址，当A接收到这个reply后，A就会跳出IP地址冲突的警告，当然B也会有警告。 因此用ARP欺骗可以来伪造这个ARPreply，从而使目标一直遭受IP地址冲突警告的困扰。 三、阻止目标的数据包通过网关 比如在一个局域网内通过网关上网，那么连接外部的计算机上的ARP缓存中就存在网关IP-MAC对应记录。如果，该记录被更改，那么该计算机向外发送的数据包总是发送到了错误的网关硬件地址上，这样，该计算机就不能够上网了。这里也主要是通过ARP欺骗进行的。有两种办法达到这样的目的。 1、向目标发送伪造的ARP应答数据包，其中发送方的IP地址为网关的地址，而MAC地址则为一个伪造的地址。当目标接收到该ARP包，那么就更新自身的ARP缓存。如果该欺骗一直持续下去，那么目标的网关缓存一直是一个被伪造的错误记录。当然，如果有些了解的人查看ARP-a，就知

道问题所在了。 2、这种方法非常狠，欺骗网关。向网关发送伪造的ARP应答数据包，其中发送方的IP地址为目标的IP地址，而MAC地址则为一个伪造的地址。这样，网关上的目标ARP记录就是一个错误的，网关发送给目标的数据报都是使用了错误的MAC地址。这种情况下，目标能够发送数据到网关，却不能接收到网关的任何数据。同时，目标自己查看ARP-a却看不出任何问题来。 四、通过ARP检测混杂模式节点 在混杂模式中，网卡进行包过滤不同于普通模式。本来在普通模式下，只有本地地址的数据包或者广播（多播等）才会被网卡提交给系统核心，否则的话，这些数据包就直接被网卡抛弃。现在，混合模式让所有经过的数据包都传递给系统核心，然后被sniffer等程序利用。 通过特殊设计的ARP请求可以用来在一定程度上检测处于混杂模式的节点，比如对网络中的每个节点都发送MAC地址为FF-FF-FF-FF-FF-FE的ARP请求。对于网卡来说这不是一个广播地址（FF-FF-FF-FF-FF-FF），所以处于普通模式的节点就会直接抛弃该数据包，但是多数操作系统核心都认为这是一个广播地址，如果有一般的sniffer程序存在，并设置网卡为混杂模式，那么系统核心就会作出应答，这样就可以判断这些节点是否存在嗅探器了。 可以查看，很多基于ARP的攻击都是通过ARP欺骗实现的。至于ARP欺骗的防范，还是尽可能使用静态的ARP.对于WIN，使用arp-s来进行静态ARP的设置。当然，如果能够完全使用静态的IP MAC对应，就更好了，因为静态的ARP缓存只是相对的。 当然，可以有一些方法来实现ARP欺骗的检测。设置一个ARP的嗅探器，其中维护着一个本地网络的IP-MAC地址的静态对应表，查看所有经过

的ARP数据，并检查其中的IP-MAC对应关系，如果捕获的IP-MAC对应关系和维护的静态对应关系对应不上，那么就表明是一个欺骗的ARP数据包了。 一个ARP数据包发送程序源代码和编译好的EXE程序可以参考ARPSender程序。注意：需要先安装WinPcap. 