cisco中的ARP命令应用介绍 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/243/2021_2022_cisco_E4_B8_AD_E7_9A_c101_243482.htm 最近一段时间，arp欺骗病毒十分猖獗，经常造成局网内主机断网。 从影响网络连接通畅的方式来看，ARP欺骗分为二种，一种是对路由器ARP表的欺骗；另一种是对内网PC的网关欺骗。 第一种ARP欺骗的原理是截获网关数据。它通知路由器一系列错误的内网MAC地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在路由器中，结果路由器的所有数据只能发送给错误的MAC地址，造成正常PC无法收到信息。第二种ARP欺骗的原理是伪造网关。它的原理是建立假网关，让被它欺骗的PC向假网关发数据，而不是通过正常的路由器途径上网。在PC看来，就是上不了网了，“ 网络掉线了 ”。 一般来说，ARP欺骗攻击的后果非常严重，大多数情况下会造成大面积掉线。 有经验的网关会利用arp命令来查找发出arp欺骗包的主机，然后采取相应的措施。但这些都是亡羊补牢的办法，能不能把防范做在前面，让那些中毒的主机无所作为呢？ 其实，cisco也有类似的命令，能够在有arp欺骗的情况下保护网关和其它主机，使网络得以畅通。 命令格式： arp IP add mac arpa intID，比如： arp 10.1.1.222 0000.ac01.2ca9 arpa fastethernet 3/19 它的作用相当于：在快速以太3/19口上，能与它连接的只能是1001.1.222，mac地址只能是0000.ac01.2ca9 ，其它一律拒绝。 在汇聚和接入交换机之间，通过这第条命令两端互相绑定对端的ip和mac地址，这样可以防止接入交换机下的pc中毒后发出虚假的arp信息，导致汇聚和接入交换机之间的通信

异常。比如汇聚在请求对端接入交换机的mac地址时，pc首先发出了回应也就是以接入交换机的管理ip和自己的（或者伪装的）mac封装了arp reply那么汇聚的arp表就会出现错误，导致整个接入交换机下的用户无法上网，这也是一种arp欺骗。利用了上面的命令就可以将汇聚和接入交换机的 arp条目固化，防止出现上述情况。 同理，在接入层交换机上做出绑定，那么当接入交换机请求目的主机的mac时，会直接从自己的固化arp表中去查找，而不会再向整个网络发布arp广播，这样即使有arp欺骗的主机存在，它也不会有向整个网络发难的机会。 