ARP

一．简介

ARP，即地址解析协议，实现通过 IP 地址得知其物理地址。在 TCP/IP 网络环境下，每个主机都分配了一个 32 位的 IP 地址，这种互联网地址是在网际范围标识主机的一种逻辑地址。为了让报文在物理网路上传送，必须知道对方目的主机的物理地址。这样就存在把 IP 地址变换成物理地址的地址转换问题。以以太网环境为例，为了正确地向目的主机传送报文，必须把目的主机的 32 位 IP 地址转换成为 48 位以太网的地址。这就需要在互连层有一组服务将 IP 地址转换为相应物理地址，这组协议就是 ARP 协议。另有电子防翻滚系统也称为 ARP。

二．基本功能

在以太网协议中规定，同一局域网中的一台主机要和另一台主机进行直接通信，必须要知道目标主机的 MAC 地址。而在 TCP/IP 协议栈中，网络层和传输层只关心目标主机的 IP 地址。这就导致在以太网中使用 IP 协议时，数据链路层的以太网协议接到上层 IP 协议提供的数据中，只包含目的主机的 IP 地址。于是需要一种方法，根据目的主机的 IP 地址，获得其 MAC 地址。这就是 ARP 协议要做的事情。所谓地址解析（address resolution）就是主机在发送帧前将目标 IP 地址转换成目标 MAC 地址的过程。

另外，当发送主机和目的主机不在同一个局域网中时，即便知道目的主机的 MAC 地址，两者也不能直接通信，必须经过路由转发才可以。所以此时，发送主机通过 ARP 协议获得的将不是目的主机的真实 MAC 地址，而是一台可以通往局域网外的路由器的某个端口的 MAC 地址。于是此后发送主机发往目的主机的所有帧，都将发往该路由器，通过它向外发送。这种情况称为 ARP 代理（ARP Proxy）。

三．工作原理

当一个基于 TCP/IP 的应用程序需要从一台主机发送数据给另一台主机时，它把信息分割并封装成包，附上目的主机的 IP 地址。然后，寻找 IP 地址到实际 MAC 地址的映射，这需要发送 ARP 广播消息。当 ARP 找到了目的主机 MAC 地址后，就可以形成待发送帧的完整以太网帧头。最后，协议栈将 IP 包封装到以太网帧中进行传送。

如图 1 所示，描述了 ARP 广播过程。

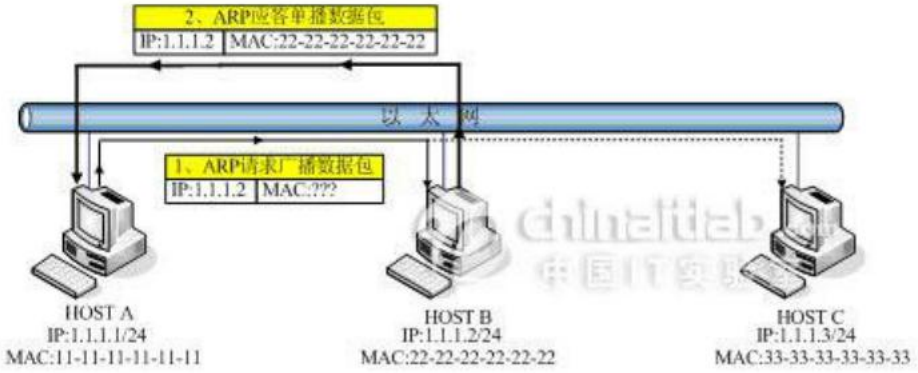
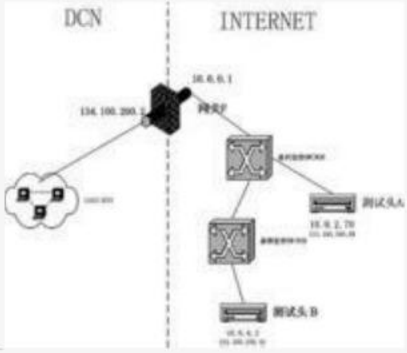


图 1　ARP 广播

在图 1 中，当主机 A 要和主机 B 通信（如主机 A Ping 主机 B）时。主机 A 会先检查其 ARP 缓存内是否有主机 B 的 MAC 地址。如果没有，主机 A 会发送一个 ARP 请求广播包，此包内包含着其欲与之通信的主机的 IP 地址，也就是主机 B 的 IP 地址。当主机 B 收到此广播后，会将自己的 MAC 地址利用 ARP 响应包传给主机 A，并更新自己的 ARP 缓存，也就是同时将主机 A 的 IP 地址/MAC 地址对保存起来，以供后面使用。主机 A 在得到主机 B 的 MAC 地址后，就可以与主机 B 通信了。同时，主机 A 也将主机 B 的 IP 地址/MAC 地址对保存在自己的 ARP 缓存内。



ARP

在每台安装有 TCP/IP 协议的电脑里都有一个 ARP 缓存表，表里的 IP 地址与 MAC 地址是一一对应的。

ARP 工作原理

以主机 A（192.168.1.5）向主机 B（192.168.1.1）发送数据为例。当发送数据时，主机 A 会在自己的 ARP 缓存表中寻找是否有目标 IP 地址。如果找到了，也就知道了目标 MAC 地址，直接把目标 MAC 地址写入帧里面发送就可以了；如果在 ARP 缓存表中没有找到目标 IP 地址，主机 A 就会在网络上发送一个广播，A 主机 MAC 地址是“主机 A 的 MAC 地址”，这表示向同一网段内的所有主机发出这样的询问：“我是 192.168.1.5，我的硬件地址是″主机 A 的 MAC 地址″.请问 IP 地址为 192.168.1.1 的 MAC 地址是什么？”网络上其他主机并不响应 ARP 询问，只有主机 B 接收到这个帧时，才向主机 A 做出这样的回应：“192.168.1.1 的 MAC 地址是 00-aa-00-62-c6-09”。这样，主机 A 就知道了主机 B 的 MAC 地址，它就可以向主机 B 发送信息了。同时 A 和 B 还同时都更新了自己的 ARP 缓存表（因为 A 在询问的时候把自己的 IP 和 MAC 地址一起告诉了 B），下次 A 再向主机 B 或者 B 向 A 发送信息时，直接从各自的 ARP 缓存表里查找就可以了。ARP 缓存表采用了老化机制（即设置了生存时间 TTL），在一段时间内（一般 15 到 20 分钟）如果表中的某一行没有使用，就会被删除，这样可以大大减少 ARP 缓存表的长度，加快查询速度。

ARP 攻击就是通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗，能够在网络中产生大量的 ARP 通信量使网络阻塞，攻击者只要持续不断的发出伪造的 ARP 响应包就能更改目标主机 ARP 缓存中的 IP-MAC 条目，造成网络中断或中间人攻击。

ARP 攻击主要是存在于局域网网络中，局域网中若有一个人感染 ARP 木马，则感染该 ARP 木马的系统将会试图通过“ARP 欺骗”手段截获所在网络内其它计算机的通信信息，并因此造成网内其它计算机的通信故障。

RARP 的工作原理：

1. 发送主机发送一个本地的 RARP 广播，在此广播包中，声明自己的 MAC 地址并且请求任何收到此请求的 RARP 服务器分配一个 IP 地址；

2． 本地网段上的 RARP 服务器收到此请求后，检查其 RARP 列表，查找该 MAC 地址对应的 IP 地址；

3． 如果存在，RARP 服务器就给源主机发送一个响应数据包并将此 IP 地址提供给对方主机使用；

4． 如果不存在，RARP 服务器对此不做任何的响应；

5． 源主机收到从 RARP 服务器的响应信息，就利用得到的 IP 地址进行通讯；如果一直没有收到 RARP 服务器的响应信息，表示初始化失败。

6.如果在第 1-3 中被 ARP 病毒攻击，则服务器做出的反映就会被占用，源主机同样得不到 RARP 服务器的响应信息，此时并不是服务器没有响应而是服务器返回的源主机的 IP 被占用。

ARP 报文格式

ARP 报文被封装在以太网帧头部中传输，如图 2 所示，是 ARP 请求协议报文头部格式。

图 2 ARP 请求协议报文头部格式

图 2 中黄色的部分是以太网（这里是 Ethernet II 类型）的帧头部。其中，第一个字段是广播类型的 MAC 地址：0XFF-FF-FF-FF-FF-FF，其目标是网络上的所有主机。第二个字段是源 MAC 地址，即请求地址解析的主机 MAC 地址。第三个字段是协议类型，这里用 0X0806 代表封装的上层协议是 ARP 协议。 接下来是 ARP 协议报文部分。其中各个字段的含义如下：

硬件类型：表明 ARP 实现在何种类型的网络上。

协议类型：代表解析协议（上层协议）。这里，一般是 0800，即 IP。

硬件地址长度：MAC 地址长度，此处为 6 个字节。

协议地址长度：IP 地址长度，此处为 4 个字节。

操作类型：代表 ARP 数据包类型。0 表示 ARP 请求数据包，1 表示 ARP 应答数据包。

源 MAC 地址：发送端 MAC 地址。

源 IP 地址：代表发送端协议地址（IP 地址）。

目标 MAC 地址：目的端 MAC 地址（待填充）。

目标 IP 地址：代表目的端协议地址（IP 地址）。

ARP 应答协议报文和 ARP 请求协议报文类似。不同的是，此时，以太网帧头部的目标 MAC 地址为发送 ARP 地址解析请求的主机的 MAC 地址，而源 MAC 地址为被解析的主机的 MAC 地址。同时，操作类型字段为 1，表示 ARP 应答数据包，目标 MAC 地址字段被填充以目标 MAC 地址。

四.地址解析报文封装

ARP/RARP 报文是作为普通数据直接封装在物理帧(以太网帧)中进行传输的，ARP/RARP 报文封装在以太网物理帧中的格式如下。

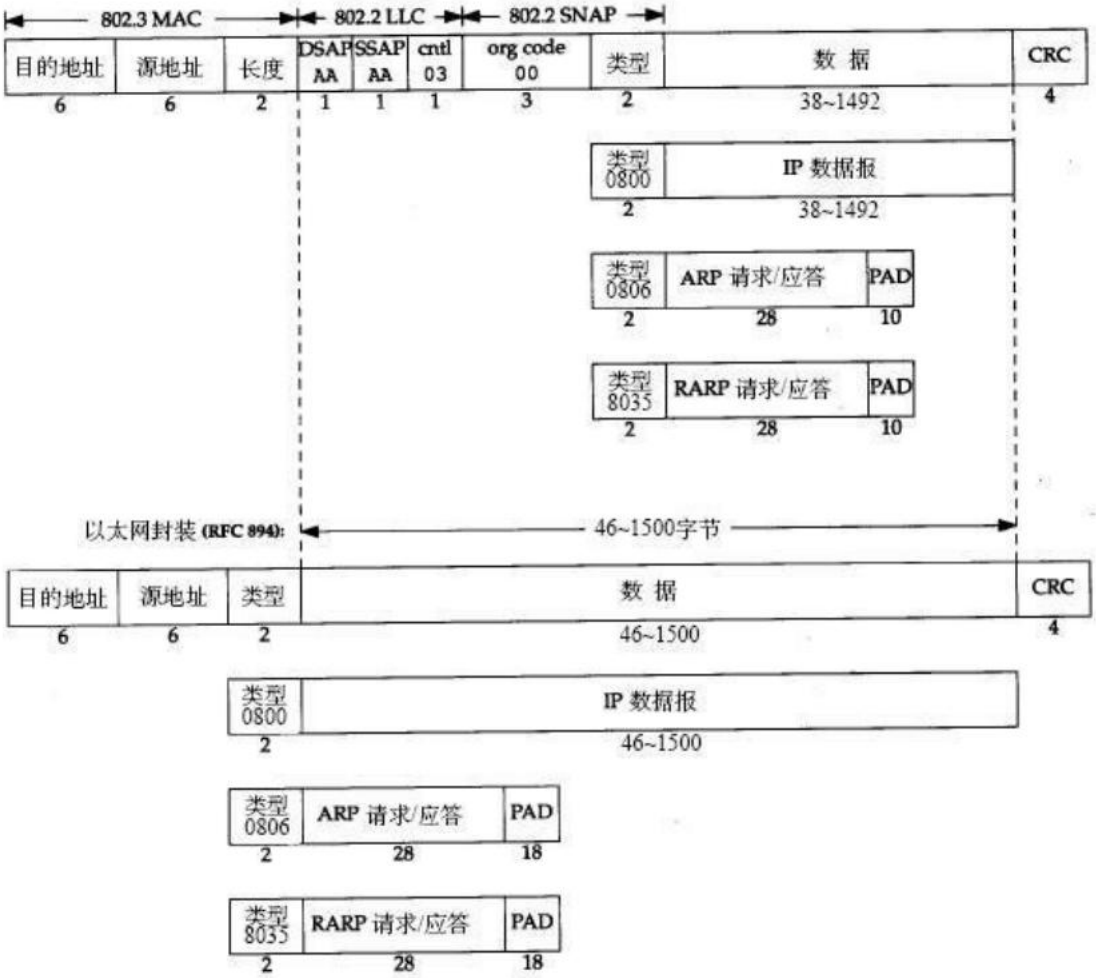
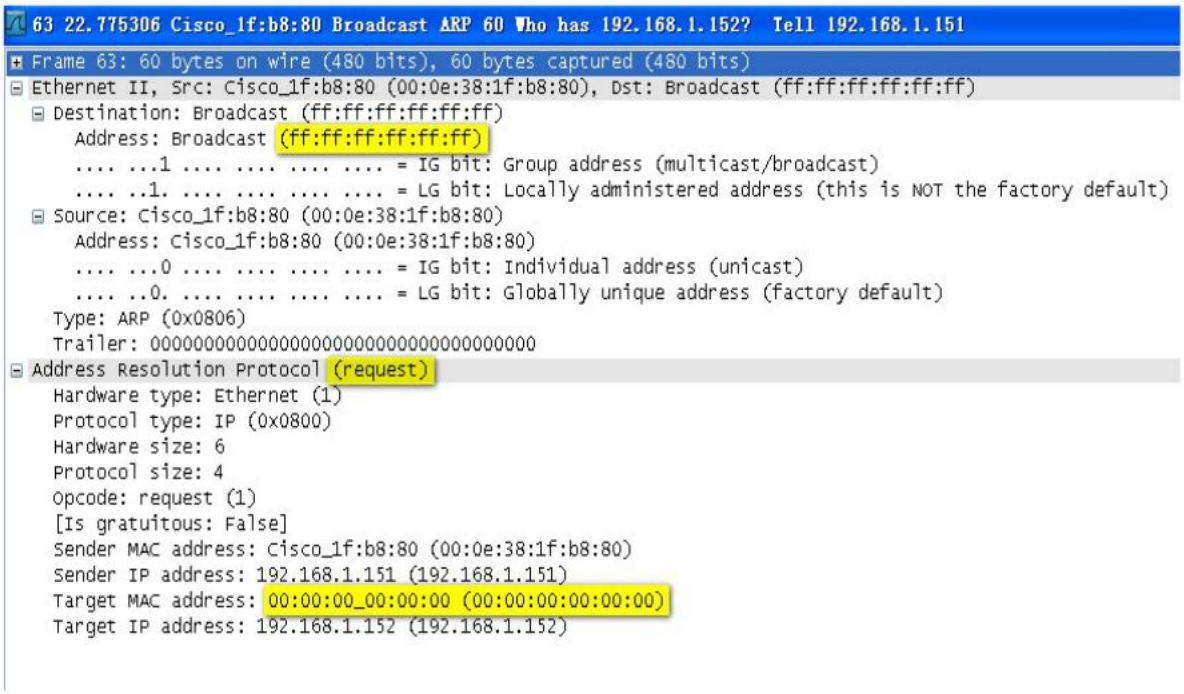
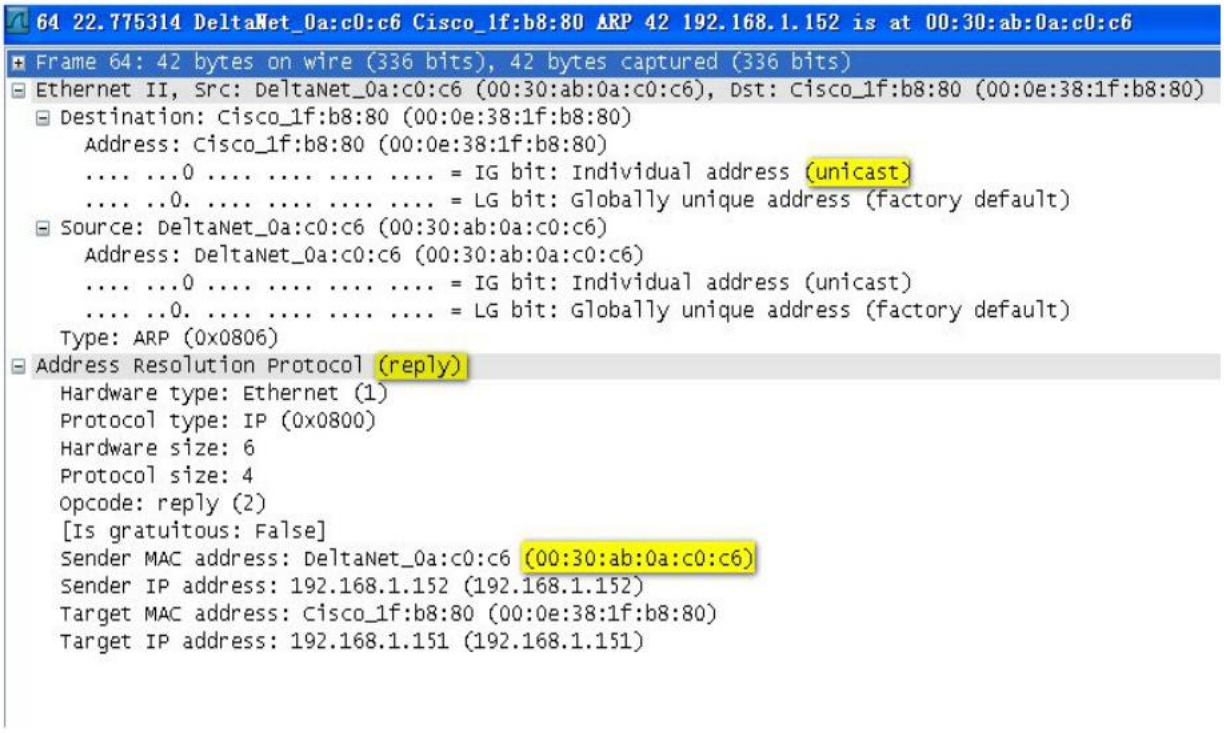


图2-1 IEEE 802.2/802.3（RFC 1042）和以太网的封装格式（RFC 894）

以太网帧的封装格式

0x0806：表示 ARP 类型，0X8035 表示 RARP 类型。ARP/RARP 作为普通数据放在数据区，由于它（ARP/RARP 报文）只有 28 字节，后面必须增加 18 个字节的填充 PAD,以达到以太网帧的最小长度要求（46 字节）。





四．**RARP** 反向地址解析协议

反向地址解析协议用于一种特殊情况，如果站点被初始化后，只有自己的物理网络地址而没有 IP 地址，则它可以通过 RARP 协议，并发出广播请求，征求自己的 IP 地址，而 RARP 服务器则负责回答。这样无 IP 的站点可以通过 RARP 协议取得自己的 IP 地址，这个地址在下一次系统重新开始以前都有效，不用连续广播请求。RARP 广泛用于获取无盘工作站的 IP 地址。

五．**ARP** 缓存表查看方法

ARP 缓存表是可以查看的，也可以添加和修改。在命令提示符下，输入“arp -a”就可以查看 ARP 缓存表中的内容了，如附图所示。

arp -a

用“arp -d”命令可以删除 ARP 表中所有的内容；

用“arp -d +空格+〈指定 ip 地址〉” 可以删除指定 ip 所在行的内容

用“arp -s”可以手动在 ARP 表中指定 IP 地址与 MAC 地址的对应，类型为 static(静态)，静态 ARP 缓存除非手动清除，否则不会丢失。无论是静态还是动态 ARP 缓存，重启启动计算机后都会丢失。

六．ARP 欺骗

其实，此起彼伏的瞬间掉线或大面积的断网大都是 ARP 欺骗在作怪。ARP 欺骗攻击已经成了破坏网吧经营的罪魁祸首，是网吧老板和网管员的心腹大患。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。有些网管员对此不甚了解，出现故障时，认为 PC 没有问题，交换机没掉线的“本事”，电信也不承认宽带故障。而且如果第一种 ARP 欺骗发生时，只要重启路由器，网络就能全面恢复，那问题一定是在路由器了。为此，宽带路由器背了不少“黑锅”。作为网吧路由器的厂家，对防范 ARP 欺骗不得已做了不少份内、份外的工作。一、在宽带路由器中把所有 PC 的 IP-MAC 输入到一个静态表中，这叫路由器 IP-MAC 绑定。二、力劝网管员在内网所有 PC 上设置网关的静态 ARP 信息，这叫 PC 机 IP-MAC 绑定。一般厂家要求两个工作都要做，称其为 IP-MAC 双向绑定。显示和修改“地址解析协议”(ARP) 所使用的到以太网的 IP 或令牌环物理地址翻译表。该命令只有在安装了 TCP/IP 协议之后才可用。

```
arp -a [inet_addr] [-N [if_addr]
arp
arp -d inet_addr [if_addr]
arp -s inet_addr ether_addr [if_addr]
```

参数

-a

通过询问 TCP/IP 显示当前 ARP 项。如果指定了 inet_addr，则只显示指定计算机的 IP 和物理地址。

-g

与 -a 相同。

inet_addr

以加点的十进制标记指定 IP 地址。

-N

显示由 if_addr 指定的网络界面 ARP 项。

if_addr

指定需要修改其地址转换表接口的 IP 地址（如果有的话）。如果不存在，将使用第一个可适用的接口。

-d

删除由 inet_addr 指定的项。

-s

在 ARP 缓存中添加项，将 IP 地址 inet_addr 和物理地址 ether_addr 关联。物理地址由以连字符分隔的 6 个十六进制字节给定。使用带点的十进制标记指定 IP 地址。项是永久性的，即在超时到期后项自动从缓存删除。

ether_addr

指定物理地址。

七．遭受 ARP 攻击后现象

ARP 欺骗木马的中毒现象表现为：使用局域网时会突然掉线，过一段时间后又会恢复正常。比如客户端状态频频变红，用户频繁断网，IE 浏览器频繁出错，以及一些常用软件出现故障等。如果局域网中是通过身份认证上网的，会突然出现可认证，但不能上网的现象（无法 ping 通网关），重启机器或在 MS-DOS 窗口下运行命令 arp -d 后，又可恢复上网。

ARP 欺骗木马只需成功感染一台电脑，就可能导致整个局域网都无法上网，严重的甚至可能带来整个网络的瘫痪。该木马发作时除了会导致同一局域网内的其他用户上网出现时断时续的现象外，还会窃取用户密码。如盗取 QQ 密码、盗取各种网络游戏密码和账号去做金钱交易，盗窃网上银行账号来做非法交易活动等，这是木马的惯用伎俩，给用户造成了很大的不便和巨大的经济损失。

八．常用的维护方法

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。下面来了解以下三种方法：静态绑定、Antiarp 和具有 ARP 防护功能的路由器。

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：

Internet Address Physical Address Type

192. 168.10.1 AA-AA-AA-AA-AA-AA static(静态)

一般不绑定,在动态的情况下：

Internet Address Physical Address Type

192. 168.10.1 AA-AA-AA-AA-AA-AA dynamic(动态)

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！

3. 2 使用 ARP 防护软件

目前关于 ARP 类的防护软件出的比较多了，大家使用比较常用的 ARP 工具主要是欣向 ARP 工具,Antiarp 等。它们除了本身来检测出 ARP 攻击外，防护的工作原理是一定频率向网络广播正确的 ARP 信息。我们还是来简单说下这两个小工具。

3. 2.1 欣向 ARP 工具

俺使用了该工具，它有 5 个功能：

A. IP/MAC 清单

选择网卡。如果是单网卡不需要设置。如果是多网卡需要设置连接内网的那块网卡。

IP/MAC 扫描。这里会扫描目前网络中所有的机器的 IP 与 MAC 地址。请在内网运行正常时扫描，因为这个表格将作为对之后 ARP 的参照。

之后的功能都需要这个表格的支持，如果出现提示无法获取 IP 或 MAC 时，就说明这里的表格里面没有相应的数据。

B. ARP 欺骗检测

这个功能会一直检测内网是否有 PC 冒充表格内的 IP。你可以把主要的 IP 设到检测表格里面，例如，路由器，电影服务器，等需要内网机器访问的机器 IP。

(补充)“ARP 欺骗记录”表如何理解：

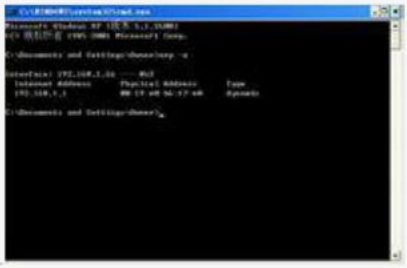
“Time”：发现问题时的时间；

“sender”：发送欺骗信息的 IP 或 MAC；

“Repeat”：欺诈信息发送的次数；

“ARP info”：是指发送欺骗信息的具体内容.如下面例子：

time sender Repeat ARP info 22:22:22 192.168.1.22 1433 192.168.1.1 is at 00:0e:03:22:02:e8



ARP

这条信息的意思是：在 22:22:22 的时间，检测到由 192.168.1.22 发出的欺骗信息，已经发送了 1433 次，他发送的欺骗信息的内容是：192.168.1.1 的 MAC 地址是 00:0e:03:22:02:e8。

打开检测功能，如果出现针对表内 IP 的欺骗，会出现提示。可以按照提示查到内网的 ARP 欺骗的根源。提示一句，任何机器都可以冒充其他机器发送 IP 与 MAC，所以即使提示出某个 IP 或 MAC 在发送欺骗信息，也未必是 100%的准确。所有请不要以暴力解决某些问题。

C. 主动维护

这个功能可以直接解决 ARP 欺骗的掉线问题，但是并不是理想方法。他的原理就在网络内不停的广播制定的 IP 的正确的 MAC 地址。

“制定维护对象”的表格里面就是设置需要保护的 IP。发包频率就是每秒发送多少个正确的包给网络内所有机器。强烈建议尽量少的广播 IP，尽量少的广播频率。一般设置 1 次就可以，如果没有绑定 IP 的情况下，出现 ARP 欺骗，可以设置到 50－100 次，如果还有掉线可以设置更高，即可以实现快速解决 ARP 欺骗的问题。但是想真正解决 ARP 问题，还是请参照上面绑定方法。arp

D. 欣向路由器日志

收集欣向路由器的系统日志，等功能。

E. 抓包

类似于网络分析软件的抓包，保存格式是.cap。

Antiarp

这个软件界面比较简单，以下为我收集该软件的使用方法。

A. 填入网关 IP 地址，点击[获取网关地址]将会显示出网关的 MAC 地址。点击[自动防护]即可保护当前网卡与该网关的通信不会被第三方监听。注意：如出现 ARP 欺骗提示，这说明攻击者发送了 ARP 欺骗数据包来获取网卡的数据包，如果您想追踪攻击来源请记住攻击者的 MAC 地址，利用 MAC 地址扫描器可以找出 IP 对应的 MAC 地址。

B. IP 地址冲突

如频繁的出现 IP 地址冲突，这说明攻击者频繁发送 ARP 欺骗数据包，才会出现 IP 冲突的警告，利用 Anti ARP Sniffer 可以防止此类攻击。

C. 您需要知道冲突的 MAC 地址，Windows 会记录这些错误。查看具体方法如下：

右击[我的电脑]--[管理]--点击[事件查看器]--点击[系统]--查看来源为[TcpIP]---双击事件可以看到显示地址发生冲突，并记录了该 MAC 地址，请复制该 MAC 地址并填入 Anti ARP Sniffer 的本地 MAC 地址输入框中(请注意将：转换为-)，输入完成之后点击[防护地址冲突]，为了使 MAC 地址生效请禁用本地网卡然后再启用网卡，在 CMD 命令行中输入 Ipconfig /all，查看当前 MAC 地址是否与本地 MAC 地址输入框中的 MAC 地址相符，如果更改失败请与我联系。如果成功将不再会显示地址冲突。

注意：如果您想恢复默认 MAC 地址，请点击[恢复默认],为了使 MAC 地址生效请禁用本地网卡然后再启用网卡。

具有 **ARP** 防护功能的路由器

这类路由器以前听说的很少,对于这类路由器中提到的 ARP 防护功能，其实它的原理就是定期的发送自己正确的 ARP 信息。但是路由器的这种功能对于真正意义上的攻击，是不能解决的。

ARP 的最常见的特征就是掉线，一般情况下不需要处理一定时间内可以回复正常上网，因为 ARP 欺骗是有老化时间的，过了老化时间就会自动的回复正常。现在大多数路由器都会在很短时间内不停广播自己的正确 ARP 信息，使受骗的主机回复正常。但是如果出现攻击性 ARP 欺骗(其实就是时间很短的量很大的欺骗 ARP，1 秒有个几百上千的)，它是不断的发起 ARP 欺骗包来阻止内网机器上网，即使路由器不断广播正确的包也会被他大量的错误信息给淹没。

可能你会有疑问：我们也可以发送比欺骗者更多更快正确的 ARP 信息啊？如果攻击者每秒发送 1000 个 ARP 欺骗包，那我们就每秒发送 1500 个正确的 ARP 信息！

面对上面的疑问，我们仔细想想，如果网络拓扑很大，网络中接了很多网络设备和主机，大量的设备都去处理这些广播信息，那网络使用起来好不爽，再说了会影响到我们工作和学习。ARP 广播会造成网络资源的浪费和占

用。如果该网络出了问题，我们抓包分析，数据包中也会出现很多这类 ARP 广播包，对分析也会造成一定的影响。

2.3 ARP 缓冲区

为了节省 ARP 缓冲区内存，被解析过的 ARP 条目的寿命都是有限的。如果一段时间内该条目没有被参考过，则条目被自动删除。在工作站 PC 的 Windows 环境中，ARP 条目的寿命是 2 分钟，在大部分 Cisco 交换机中，该值是 5 分钟。

在工作站 PC 的 Windows 环境中，可以使用命令 arp -a 查看当前的 ARP 缓存，如图 3 所示。而在路由器和交换机中可以命令 show arp 完成相同的功能，如图 4 所示。

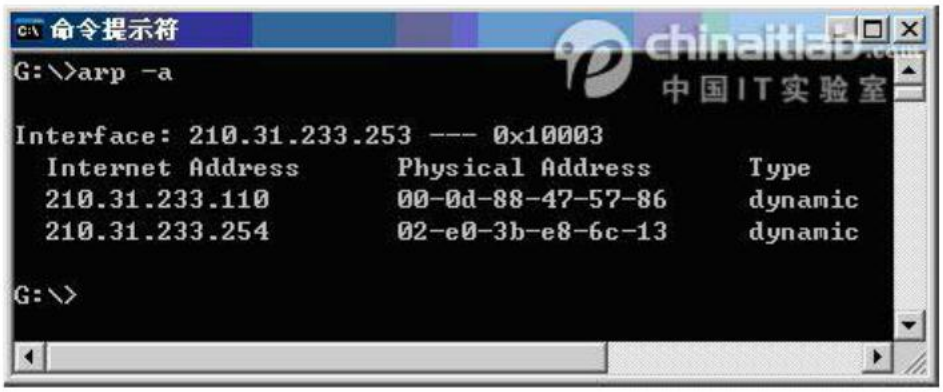


图 3 Windows 环境下，命令 arp -a 的输出

```
Router#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  210.31.224.233        0    0060.94b9.d14b  ARPA   FastEthernet0/1
Internet  210.31.224.186        0    0800.20a9.a544  ARPA   FastEthernet0/1
Internet  210.31.221.254        0    00e0.4ce0.eadb  ARPA   FastEthernet1/0
Internet  210.31.221.253        -    000b.fdd2.9c91  ARPA   FastEthernet1/0
Internet  210.31.224.254        -    000b.fdd2.9c82  ARPA   FastEthernet0/1
Internet  61.240.133.177        0    00e0.fc04.c541  ARPA   FastEthernet0/0
Internet  61.240.133.178        -    000b.fdd2.9c81  ARPA   FastEthernet0/0
Router#
```

图 4 路由器中 show arp 命令的输出

注意：ARP 不能通过 IP 路由器发送广播，所以不能用来确定远程网络设备的硬件地址。对于目标主机位于远程网络的情况，IP 利用 ARP 确定默认网关（路由器）的硬件地址，并将数据包发到默认网关，由路由器按它自己的方式转发数据包。

3　反向 ARP

反向 ARP（Reverse ARP，RARP）用于把物理地址（MAC 地址）转换到对应的 IP 地址。例如，在无盘工作站启动的时候，因为无法从自身的操作系统获得自己的 IP 地址配置信息。这时，无盘工作站可发送广播请求获得自己的 IP 地址信息，而 RARP 服务器则响应 IP 请求消息一为无盘工作站分配 1 个未用的 IP 地址（通过发送 RARP 应答包）。

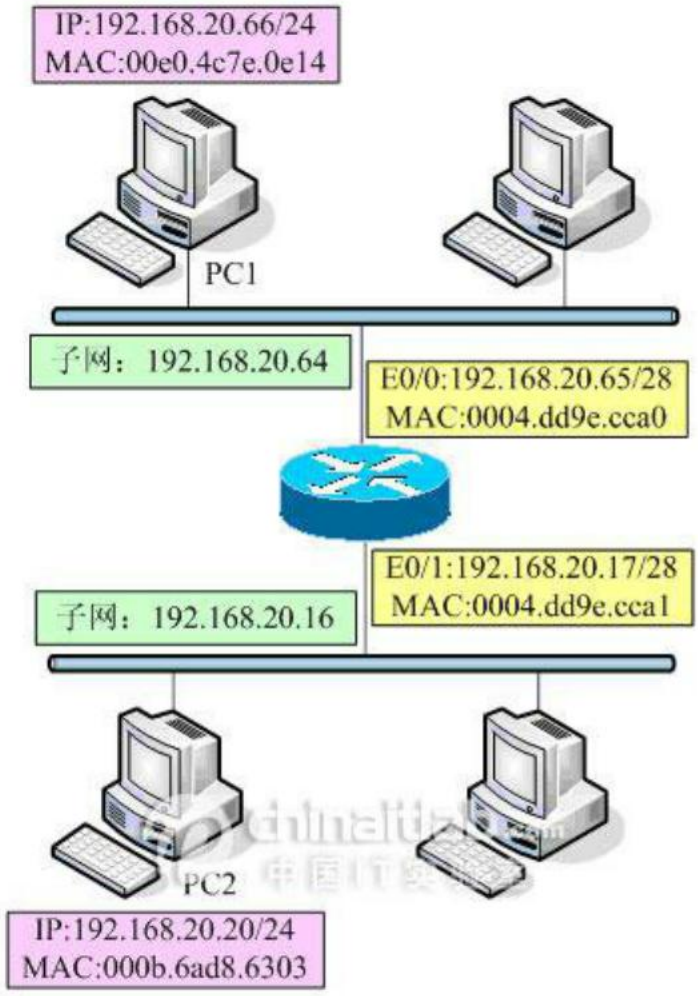
反向 ARP（RARP）在很大程度上已被 BOOTP、DHCP 所替代，后面这两种协议对 RARP 的改进是可以提供除了 IP 地址外的其它更多的信息，如默认网关、DNS 服务器的 IP 地址等信息。

4　代理 ARP

代理 ARP（PROXY ARP）也被称作混杂 ARP（Promiscuous ARP）（RFC 925、1027）一般被像路由器这样的设备使用--用来代替处于另一个网段的主机回答本网段主机的 ARP 请求。

下面是代理 ARP 的应用之一，如图 5 所示，主机 PC1（192.168.20.66/24）需要向主机 PC2（192.168.20.20/24）发送报文，因为主机 PC1 不知道子网的存在且和目标主机 PC2 在同一主网络网段，所以主机 PC1 将发送 ARP 请求广播报文请求 192.168.20.20 的 MAC 地址。这时，路由器将识别出报文的目标地址属于另一个子网（注意，路由器的接口 IP 地址配置的是 28 位的掩码），因此向请求主机回复自己的硬件地址（0004.dd9e.cca0）。之后，PC1 将发往 PC2 的数据包都发往 MAC 地址 0004.dd9e.cca0（路由器的接口 E0/0），由路由器将数据包转发到目标主机 PC2。（接下来路由器将为 PC2 做同样的代理发送数据包的工作）。这种 ARP 使得子网化网络拓扑对于主机来说时透明的（或者可以说是路由器以一个不真实的 PC2 的 MAC 地址欺骗了源主机 PC1）。

图 5　代理 ARP



5　无故 ARP

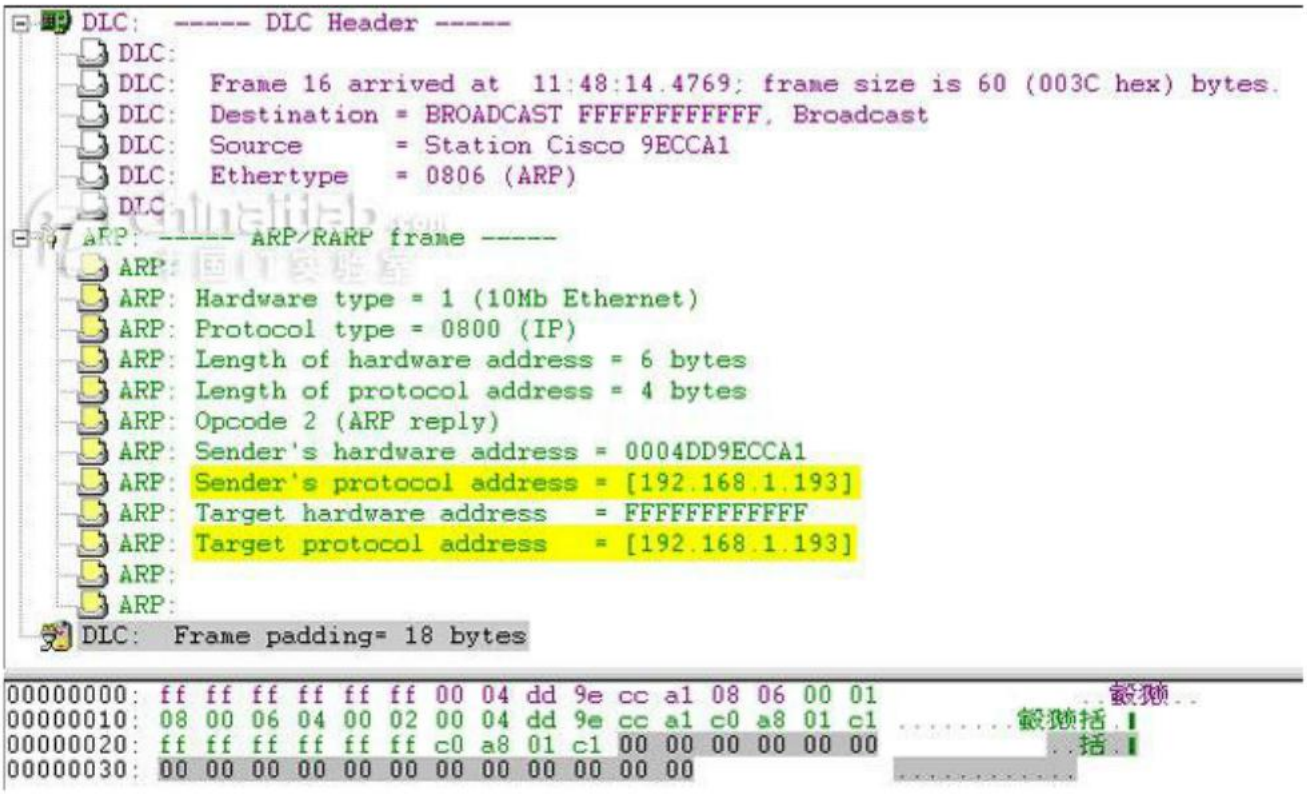
无故（Gratuitous ARP，GARP）ARP 也称为无为 ARP。主机有时会使用自己的 IP 地址作为目标地址发送 ARP 请求。这种 ARP 请求称为无故 ARP，GARP，主要有两个用途：

（1）检查重复地址（如果收到 ARP 响应表明存在重复地址）。

（2）用于通告一个新的数据链路标识。当一个设备收到一个 arp 请求时，发现 arp 缓冲区中已有发送者的 IP 地址，则更新此 IP 地址的 MAC 地址条目。

如图 6 所示，显示了一台 Cisco 路由器在其加电启动后、引导过程中向网络宣布自己的一个以太网接口（Ethernet 0）的 MAC 地址以及 IP 地址的包。

图 6　无故 ARP



从图中可以看出，这个 ARP 包的类型编码是 2，代表一个 ARP 应答消息（但是之前并没有对此 IP 的 ARP 请求消息）。这个 ARP 包的源硬件地址（MAC 地址）是路由器的这个接口的 MAC 地址，目标硬件地址（MAC 地址）使用的是广播地址（FF-FF-FF-FF-FF-FF）；而源和目标协议地址（IP 地址）都是此接口自身的 IP 地址。此 ARP 包用于设备（路由器）向网络宣告自身的 IP 地址和 MAC 地址映射，也用于检查是否有重复（冲突）的 IP 地址。

MAC 地址欺骗防护

在数据链路层中，用来标识节点的就是其 MAC 地址。它是局域网中进行网络通信的基础。但是在平常的网络通信操作中，都不是以 MAC 地址来指定目标节点的，而是以 IP 地址或 NetBIOS 名称。这样就存在一个 IP 地址与 MAC 地址的对应关系，它们之间的相互解析是通过 ARP（Address Resolution Protocol，地址解析协议）或 RARP（Reverse Address Resolution Protocol，反向地址解析协议）协议进行的：ARP 负责由 IP 地址解析出 MAC 地址，适用于有盘网络，而 RARP 负责从 MAC 地址解析出 IP 地址，适用于无盘网络。如果修改了其中的任何一项，则可能导致找不到真正的目标节点而通信不成功。这就是两种欺骗：IP 地址欺骗和 MAC 地址欺骗。IP 地址欺骗是基于网络层的，而 MAC 地址欺骗是基于数据链路层的。在此仅介绍 MAC 地址欺骗。

10.5.1 ARP 和 RARP 协议工作原理

MAC 地址与 IP 地址是计算机网络通信中非常重要的两类地址，缺一不可。因为在 OSI/RM 网络层以上是通过 IP 地址进行寻址的，而在 OSI/RM 网络层以下则是通过 MAC 地址进行寻址的。可以说是两类地址各司其职，共同完成一个完整的计算机网络通信。当然在一些网络通信中，还可能有传输层的"端口"号参与到 IP 寻址中。

1．ARP 工作原理

前面介绍到，ARP 协议是用于由节点 IP 地址解析其 MAC 地址，然后进行局域网内部通信的。例如要与某主机连接，可以在浏览器或运行窗口中输入其 IP 地址，然而在局域网内是没有网络层的，网络中的主机设备不能识别 IP 地址，只识别 MAC 地址，所以这时就需要 ARP 协议来转换。ARP 协议的基本功能就是通过数据包中的目标节点的 IP 地址查询目标节点的 MAC 地址，以便把数据包发送到目标设备中。

ARP 的基本工作原理如下：

（1）每台主机都会根据以往在网络中与其他节点的通信，在自己的 ARP 缓存区（ARP Cache）中建立一个 ARP 列表，以表示网络中节点 IP 地址和 MAC 地址的对应关系。

【说明】ARP 缓存表采用了老化机制，在一段时间内如果表中的某一行没有使用（Windows 系统的这个时间为 2 分钟，而 Cisco 路由器的这个时间为 5 分钟），就会被删除，这样可以大大减少 ARP 缓存表的长度，加快查询速度。

（2）当源节点需要将一个数据包发送到目标节点时，会首先检查自己 ARP 列表中是否存在该包中所包含的目标节点 IP 地址对应的 MAC 地址。如果有，则直接将数据包发送到这个 MAC 地址节点上；如果没有，就向本地网段发起一个 ARP 请求的广播包，查询此 IP 地址目标节点对应的 MAC 地址。此 ARP 请求数据包里包括源节点的 IP 地址、硬件地址，以及目标节点的 IP 地址。

（3）网络中所有的节点在收到这个 ARP 请求后，会检查数据包中的目标 IP 地址是否和自己的 IP 地址一致。如果不相同就忽略此数据包；如果相同，该节点首先将源端的 MAC 地址和 IP 地址的对应表项添加到自己的 ARP 列表中。如果发现 ARP 表中已经存在该 IP 地址所对应的 MAC 地址表项信息，则将其覆盖，然后给源节点发送一个 ARP 响应数据包，告诉对方自己是它需要查找的 MAC 地址节点。

（4）源节点在收到这个 ARP 响应数据包后，将得到的目标节点的 IP 地址和 MAC 地址对应表项添加到自己的 ARP 列表中，并利用此信息开始数据的传输。如果源节点一直没有收到 ARP 响应数据包，则表示 ARP 查询失败。

2．RARP 工作原理

ARP 协议是根据 IP 地址找其对应的 MAC 地址，而 RARP 则是根据 MAC 地址找其对应 IP 地址，所以称之为"反向 ARP"。具有本地磁盘的系统引导时，一般是从磁盘上的配置文件中读取 IP 地址，然后即可直接用 ARP 协议找出与其对应的主机 MAC 地址。但是无盘机，如 X 终端或无盘工作站，启动时是通过 MAC 地址来寻址的，这时就需要通过 RARP 协议获取 IP 地址。

RARP 的基本工作原理如下：

（1）发送端发送一个本地的 RARP 广播包，在此广播包中声明自己的 MAC 地址，并且请求任何收到此请求的 RARP 服务器分配一个 IP 地址。

（2）本地网段上的 RARP 服务器收到此请求后，检查其 RARP 列表，查找该 MAC 地址对应的 IP 地址。如果存在，RARP 服务器就给源主机发送一个响应数据包，并将此 IP 地址提供给对方主机使用；如果不存在，RARP 服务器对此不做任何响应。

（3）源端在收到从 RARP 服务器来的响应信息后，利用得到的 IP 地址进行通信；如果一直没有收到 RARP 服务器的响应信息，则表示初始化失败。