链滴

ARP 协议详解

作者：Gakkiyomi2019

原文链接：https://ld246.com/article/1602496741975

来源网站：链滴

许可协议：署名-相同方式共享 4.0 国际 (CC BY-SA 4.0)

ARP协议

地址解析协议，即ARP（Address Resolution Protocol），是根据IP地址获取物理地址的一个TCP/I协议。主机发送信息时将包含目标IP地址的ARP请求广播到网络上的所有主机，并接收返回消息，以确定目标的物理地址；收到返回消息后将该IP地址和物理地址存入本机ARP缓存中并保留一定时间，次请求时直接查询ARP缓存以节约资源。地址解析协议是建立在网络中各个主机互相信任的基础上的网络上的主机可以自主发送ARP应答消息，其他主机收到应答报文时不会检测该报文的真实性就会将记入本机ARP缓存；由此攻击者就可以向某一主机发送伪ARP应答报文，使其发送的信息无法到达预的主机或到达错误的主机，这就构成了一个ARP欺骗。**ARP命令可用于查询本机ARP缓存中IP地址和AC地址的对应关系、添加或删除静态对应关系等。**

简单的来说 **arp协议就是根据ip地址获取mac地址。**

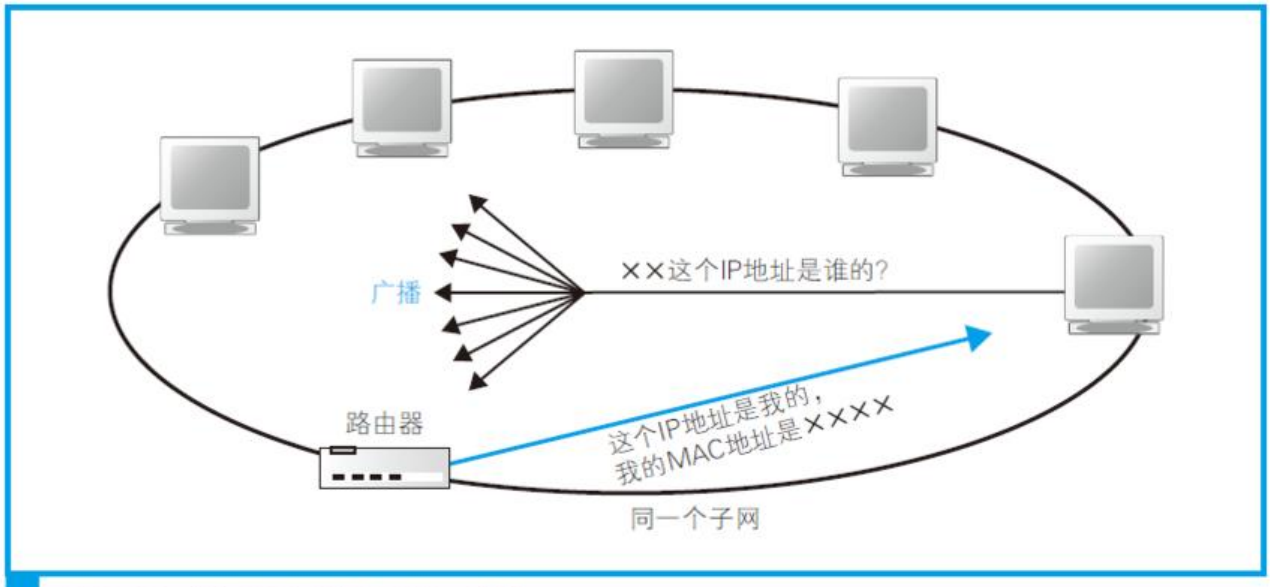


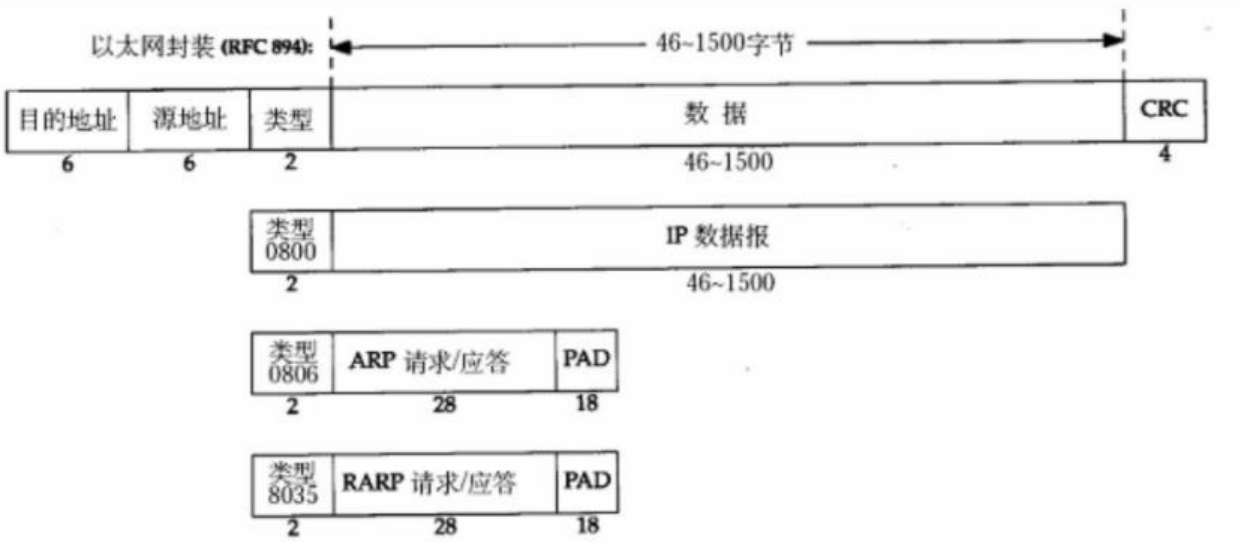
图 2.19　用 ARP 查询 MAC 地址

以太网帧格式

不管上层是什么协议什么应用，到了数据链路层都是通过以太网发送的，我们先看看以太网帧格式

所以我们想要进行网络传输一定要知道目的方的mac地址，mac地址是唯一的。这时候就需要用到ar协议通过ip地址得到mac地址。

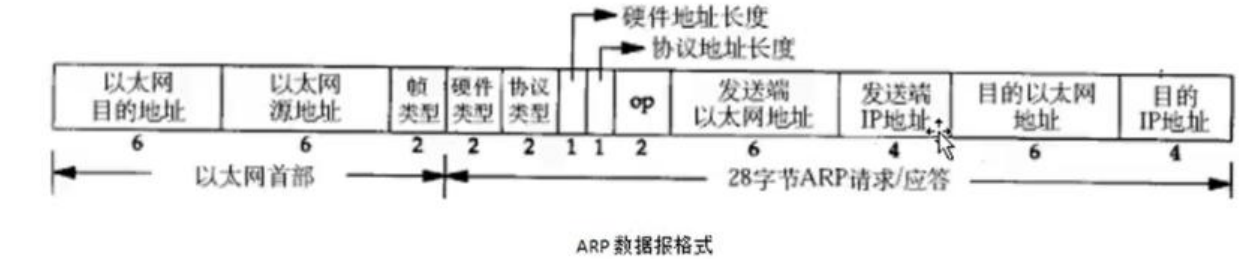
原文链接：ARP 协议详解



字段名称		长度（比特）	含　义
MAC 头部（14 字节）	接收方 MAC 地址	48	网络包接收方的 MAC 地址，在局域网中使用这一地址来传输网络包
	发送方 MAC 地址	48	网络包发送方的 MAC 地址，接收方通过它来判断是谁发送了这个包
	以太类型	16	使用的协议类型。下面是一些常见的类型，一般在 TCP/IP 通信中只使用 0800 和 0806 这两种。 0000-05DC：IEEE 802.3 0800　　：IP 协议 0806　　：ARP 协议 86DD　　IPv6

ARP报文格式

ARP 数据报的格式如下所示：



ARP 数据报格式

假设自己的mac地址为00:0c:29:0a:c4:c1　IP为192.168.1.25

原文链接：ARP 协议详解

想获取 192.168.1.33 的mac地址　00:03:21:0a:b4:a1

在发送arp请求的时候 由于不知道目的地址的mac地址，所以arp报文格式中的以太网目的地址需要充为

00:00:00:00:00:00

以太网目的地址	**以太网源地址**	**协议类型**	**发送端以太网地址**	**发送端IP地址**	**目的以太网地址**	**目的IP地址**
00:00:00:00:00:00	00:0c:29:0a:c4:c1	0806	00:0c:29:0a:c4:c1	192.168.1.25	00:00:00:00:00:00	192.168.1.33

然后再当前网段局域网中广播此arp包，每台主机都会对比目的地址ip，如果对不上就丢弃此arp包，果对上了就发送arp回包，格式一样。

192.168.1.33这台主机的arp回包

以太网目的地址	**以太网源地址**	**协议类型**	**发送端以太网地址**	**发送端IP地址**	**目的以太网地址**	**目的IP地址**
00:0c:29:0a:c4:c1	00:03:21:0a:b4:a1	0806	00:03:21:0a:b:a1	192.168.1.33	00:0c:29:0a:c4:c1	192.168.1.25

33发送的arp回包也将在局域网内广播，对不上ip的主机就会丢弃此arp包，192.168.1.25收到arp回后就得到了33的mac地址，将其填充到以太网帧的mac头部进行网络传输。

如果经过多个路由器的话，我们还需要配合路由表进行工作，这个在路由协议的时候再说。