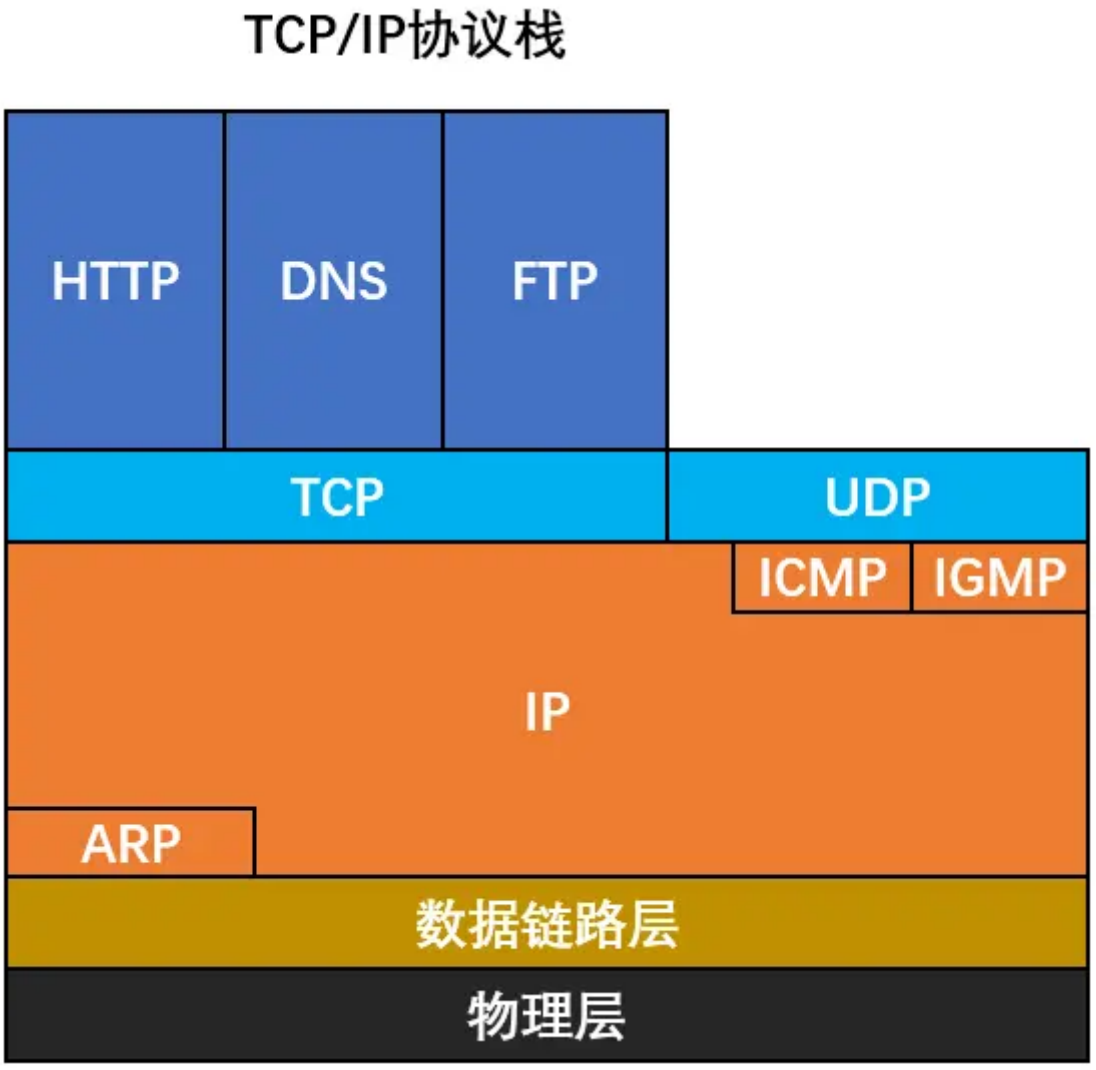
ARP协议

前言

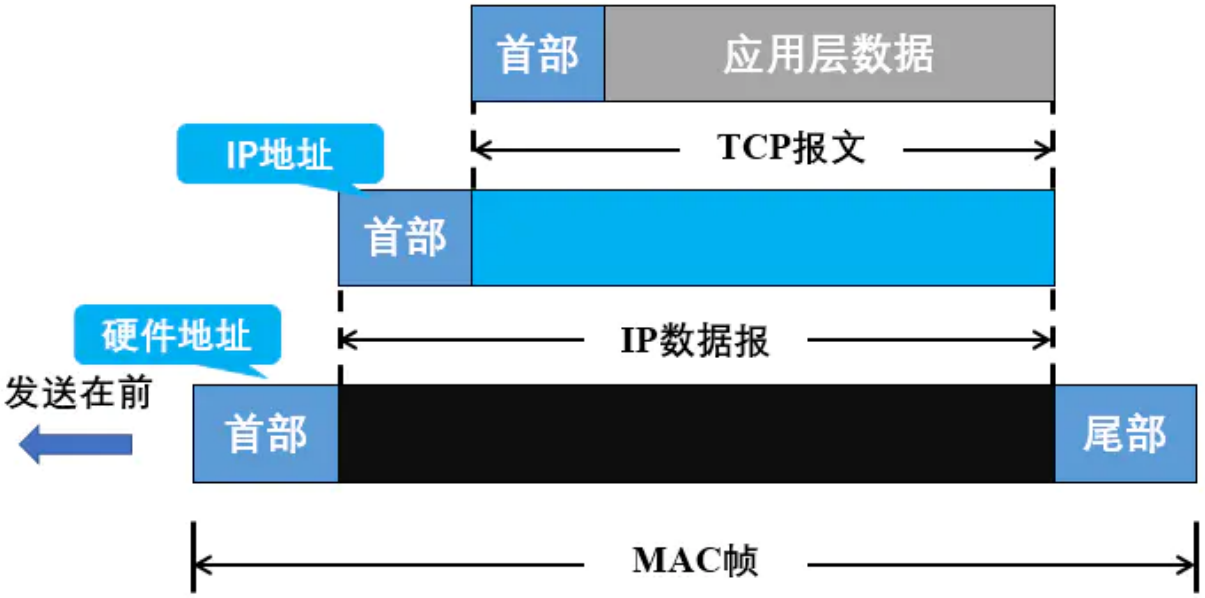
回顾TCP/IP 协议栈，在网络层中底部有一个ARP协议，由于存在网络层（IP地址）和链路层地址（硬件地址），所以需要在它们之间实现转换。这就是ARP协议的任务，所以ARP协议在数据链路层和网络层之间。



1.IP地址和硬件地址

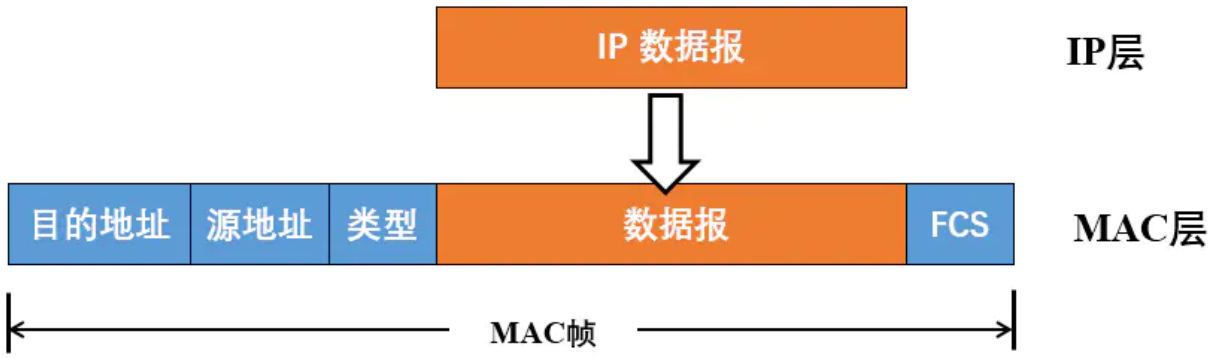
(1) **硬件地址**：在局域网中，由于硬件地址固化在网卡的ROM中，所以硬件地址常常也叫做**物理地址**。局域网中MAC帧中的源地址和目的地址都是硬件地址，所以硬件地址又称为**MAC地址**。物理地址是数据链路层和物理层使用的地址。

(2) IP地址：IP地址是网络层和以上各层使用的地址，是一种**逻辑地址**。



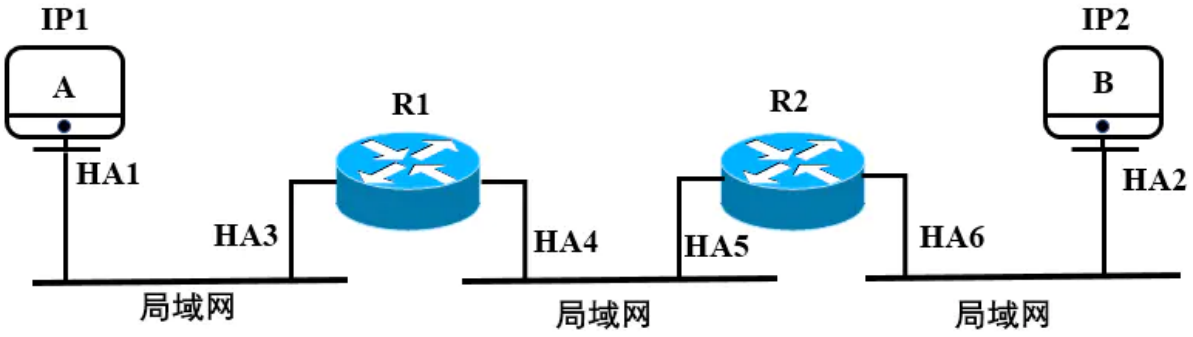
在发送数据时，数据从高层到低层，然后才到通信链路上传输。使用IP地址的IP数据报一旦交给了数据链路层，就被封装成了MAC帧。MAC帧在传送时使用的源地址和目的地址都是**硬件地址**，这两个硬件地址都写在MAC帧的首部。

一旦IP数据报放入数据链路层的MAC帧中后，整个IP数据报就成为了MAC帧的数据，因而在数据链路层看不见数据报的IP地址。



连接在通信链路上的设备（主机或路由器）在收到MAC帧时，根据MAC帧首部中的硬件地址决定收下或丢弃。只有在剥去MAC帧的首部和尾部后把MAC层的数据上交给网络层才能在IP数据报的首部中找到源IP地址和目的IP地址。

举个例子说明，如下图所示，假设主机A要和主机B通信，它们的IP地址分别为IP1和IP2，其中HA（Hard Address）表示硬件地址。



通信路径是：A——经过R1转发——再经过R2转发——B。下表给出了在不同层次、不同区间的源地址和目的地址。

	网络层		数据链路层	
	源地址	目的地址	源地址	目的地址
从A到R1	IP1	IP2	HA1	HA3
从R1到R2	IP1	IP2	HA4	HA5
从R2到B	IP1	IP2	HA6	HA2

从上表中可以看出以下几点：

> (1) **在IP层抽象的互联网中只能看到IP数据报。**虽然IP数据报要经过路由器R1和R2两次转发，但是它的首部中的源地址和目的地址始终都是IP1和IP2。

(2) **在数据链路层，只能看见MAC帧。**IP数据报封装在MAC帧中，MAC帧在不同的网络上传送时，MAC帧首部中的源地址和目的地址要发生变化。例如，开始在A和R1之间传送时，其MAC帧首部的源地址和目的地址分别为HA1和HA3，路由器R1收到此MAC帧后，在数据链路层，要丢弃原来MAC帧的首部和尾部，在转发时，要重新添加上MAC帧的首部和尾部。**MAC帧首部的这种变化，在上面的IP层上是看不见的。**

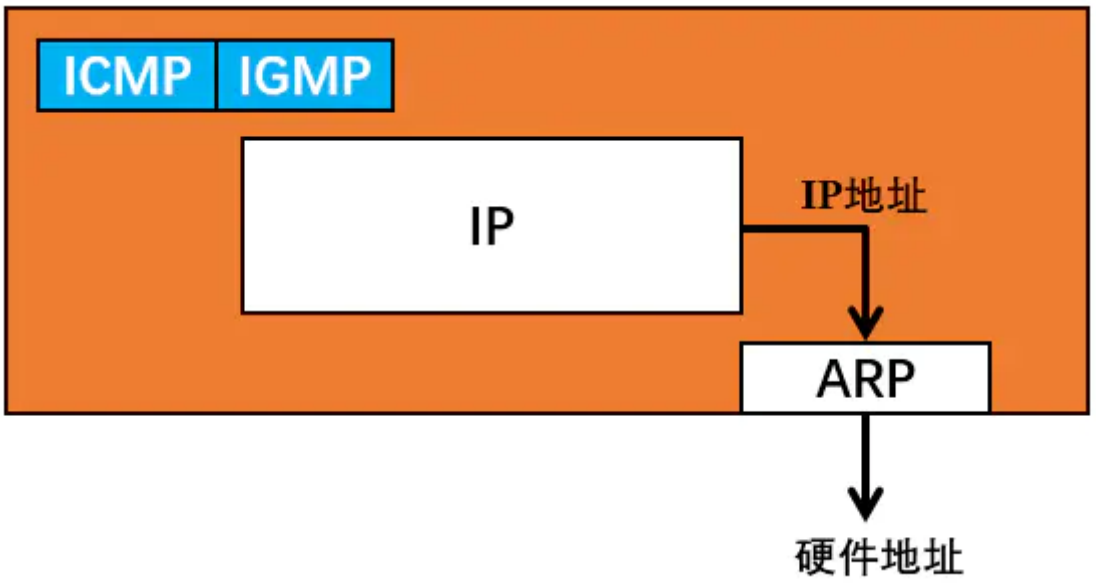
(3) **IP层抽象的互联网屏蔽了下层这些复杂的细节。**只要在网络层上讨论问题，就能够使用统一的、抽象的IP地址研究主机和主机或路由器之间的通信。

在知道了网络层和数据链路层不同区间的源地址和目的地址变化后，下面就需要了解主机或路由器怎么知道应当在MAC帧中添加什么样的硬件地址，这就是ARP协议的工作。

2.地址解析协议ARP

地址解析协议ARP（Address Resolution Protocol）其作用就是从**网络层使用的IP协议，解析出数据链路层的使用的硬件地址**，以此完成主机或路由器IP地址到MAC地址的映射。

> 由于是IP协议使用了ARP协议，所以通常将ARP协议划归网络层，认为数据链路层也可，最好是看做是跨越数据链路层和网络层边界两边的协议。



网络层使用的IP地址，但是实际网络的链路上传送数据帧时，最终必须使用网络的硬件地址。但是IP地址和硬件地址之间由于格式不同不存在简单的映射关系（IP地址有32位如IPv4，而局域网的硬件地址是48位）。

地址解析协议ARP**在主机ARP高速缓存中存放了一个从IP地址到硬件地址的映射表**，并且这个映射表还经常动态更新（新增或删除）。

IP地址	MAC地址	TTL
222.222.222.221	88-B2-2F-54-1A-0F	13:45:00
222.222.222.223	5C-66-AB-90-65-C7	13:52:00

> 表中包含一个**生存时间**（Time to Live,TTL）值，它指示了从表中删除每个映射的时间。一般过期时间是20分钟。

> 这个生存时间十分重要，设想，主机A和主机B通信，主机A中的ARP高速缓存中有主机B的IP地址和硬件地址的映射，如果主机B的网络适配器坏了，B立即更换了一块，那么B的硬件地址就变了，此时A如果还要跟B通信，使用ARP高速缓存中的硬件地址向主机B发送MAC帧，这显然是

> 无用的。如果设置了过期时间，过了生存时间，A的ARP高速缓存就会删除这个映射关系，于是A重新广播请求分组就可以得到B的新的硬件地址，就又可以和B通信了。

3.ARP工作原理

当主机A要向局域网上的某台主机B发哦送给你IP数据报时，就先在其ARP高速缓存中查看是否有主机B的IP地址，如果有，就在ARP缓存中查出其对应的硬件地址，如果查不到主机B的硬件地址，那么主机A就**自动运行ARP**，通过以下步骤查询出主机B的硬件地址：

(1) ARP进程会在本局域网上广播发送一个ARP请求分组，使用广播地址（即FF-FF-FF-FF-FF-FF）来发送这个分组。

> 请求分组包含几个字段，请求方和接收方的IP地址和MAC地址。

> 这个分组相当于向本局域中所有的主机喊了一声：我的IP地址是209.0.0.5，硬件地址是00-00-C0-15-AD-18。我想知道IP地址为209.0.0.6的主机的MAC地址。

(2) 在本局域网中的所有主机上运行的ARP进程都收到这个ARP请求分组，并检查其IP地址与ARP请求的IP地址是否一致，不匹配的主机都不会理睬这个分组，与之匹配的主机会给主机A单播一个带有其硬件地址的响应ARP分组（和请求分组格式相同）。

对于上例，IP地址为209.0.0.6的响应ARP分组就如下

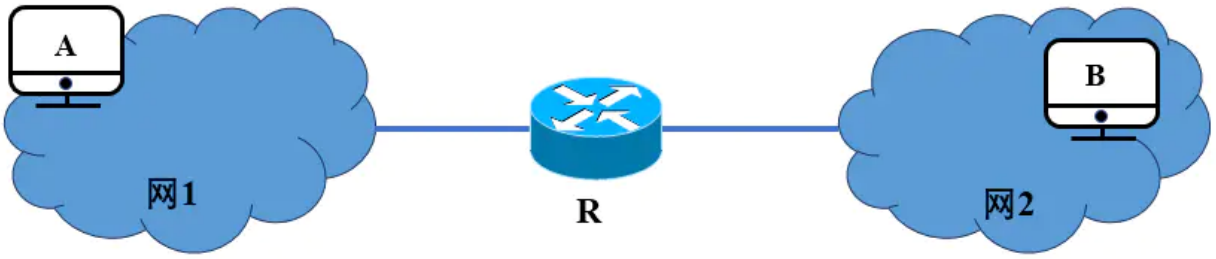
> 通常，主机B接收到ARP请求分组也会将主机A的IP地址和硬件地址映射存在自己ARP高速缓存中，因为主机A要和自己通信，自己不久也可能给它发送数据。这样可以减少网络通信量

(3) 主机A收到主机B的ARP响应分组后，就在其ARP高速缓存中写入主机B的IP地址到硬件地址的映射。

> ARP是解决同一局域网上的主机或路由器IP地址和硬件地址的映射问题。

4.不同局域网ARP协议的工作原理

如下图所示，如果要找的主机和源主机不在同一个局域网中，源主机就无法解析出另一个局域网上目的主机的硬件地址。



对于上图，实际上主机A不需要知道主机B的硬件地址，主机A发送给主机B的IP数据报首先需要通过与主机A连接在同一个局域网中上的路由器R来转发。因此主机H1这时需要把路由器R地IP地址通过ARP协议解析成硬件地址，这样就可以将IP数据报发送到路由器R。之后，R在转发表中查找到达目的IP地址的下一跳是直接交付，所以同样使用ARP协议解析出主机B的硬件地址，封装成帧发送到主机B。

ARP协议的四种典型情况：
(1) 主机发给本网络上的主机：用ARP解析目的主机的硬件地址。
(2) 主机发送给另一个网络的主机：用ARP解析本网络上一个路由器的硬件地址，之后工作是(3)或(4)。
(3) 路由器发送给本网络的主机：用ARP解析目的主机的硬件地址。
(4) 路由器发送给另一个网络的主机：用ARP找到本网络上的一个路由器的硬件地址。

5.总结


ARP
概述
地址解析协议，网络层和链路层的边界协议。
将IP地址解析成MAC地址，完成IP地址到MAC地址的映射。
主机的ARP高速缓存中存放了IP地址到MAC地址的映射表。
ARP是即插即用的，ARP表自动建立，地址解析过程自动完成。
原理
源主机广播发送ARP请求分组。
仅目的主机单播一个ARP响应分组。
源主机将ARP响应分组中的硬件地址写入ARP高速缓存中。
4种情况
主机发送给本网络上的主机。
主机发送给另一网络上的主机。
路由器发送给本网络上的主机。
路由器发送给另一网络上的主机。