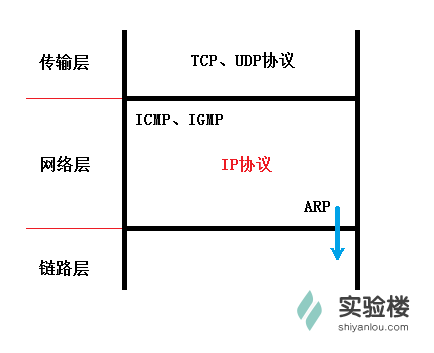
# 网络层其它协议

网络层不仅有 IP 协议，还有其它如 ARP、ICMP 等其它协议，这一节我们将对这些协议做介绍。



## 一、ARP(Address Resolution Protocol)地址解析协议

**功能**

当主机通过数据链路发送数据的时候， **IP 数据报** 会先被封装为一个 **数据帧** ，而 **MAC 地址** 会被添加到数据帧的 **报头** （链路层介绍时已讲过）。 ARP 便是在这个过程中通过目标主机的 IP 地址，查询目标主机的 MAC 地址。

**原理**

在你的电脑和路由器中都有一个 **ARP 缓存表** ，其中保存的是近期(20 分钟)与自己有过通信的主机的 IP 地址与 MAC 地址的对应关系。

ARP 缓存表使用过程：

当主机要发送一个 IP 数据报的时候，会首先查询一下自己的 ARP 缓存表；

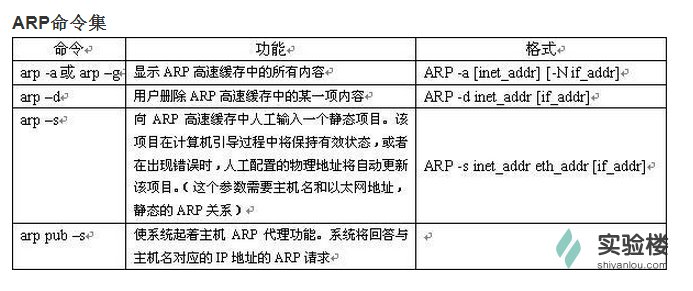
如果在 ARP 缓存表中找到对应的 MAC 地址，则将 IP 数据报封装为数据帧，把 MAC 地址放在帧首部，发送数据帧；

如果查询的 IP－MAC 值对不存在，那么主机就向网络中广播发送一个 ARP 请求数据帧，ARP 请求中包含待查询 IP 地址；

网络内所有收到 ARP 请求的主机查询自己的 IP 地址，如果发现自己符合条件，就回复一个 ARP 应答数据帧，其中包含自己的 MAC 地址；

收到 ARP 应答后，主机将其 IP - MAC 对应信息存入自己的 ARP 缓存，然后再据此封装 IP 数据报，再发送数据帧。

你可以通过命令 **arp -a** 查看 ARP 缓存表(表项记录 20 分钟超时)，这里还有其它 ARP 命令可以对缓存表做查看、修改：



**ARP 代理**

如果 ARP 请求是从一个网络上的主机发往另一个网络上的主机，那么连接这两个网络的路由器就可以回答该 ARP 请求，这个过程称作 **代理 ARP**（Proxy ARP）。

当连接这两个网络的路由器收到该 ARP 请求时，它会发现自己有通向目的主机的路径，随后它会将自己(路由器)的 MAC 地址回复给源主机。源主机会认为路由器的 MAC 地址就是目的主机的 MAC 地址，而对于随后发来的数据帧，路由器会转发到它后面真实 MAC 地址的目的主机。

两个物理网络之间的路由器可以使这两个网络彼此透明化，在这种情况下，只要路由器设置成一个 ARP 代理，以响应一个网络到另一个网络主机的 ARP 请求，两个物理网络就可以使用相同的网络号。

**ARP 欺骗**

从 ARP 代理的原理可以看出来：IP - MAC 的对应信息很容易被伪造！黑客可以伪造 ARP 应答数据帧而欺骗 ARP 请求者，从而达到截获数据的目的。

## 二、RARP(Reverse Address Resolution Protocol)逆向地址解析协议

听名字就知道，RARP 与 ARP 是相反的关系，用于将 MAC 地址转换为 IP 地址。对应于 ARP，RARP 请求以广播方式传送，而 RARP 应答一般是单播传送的。

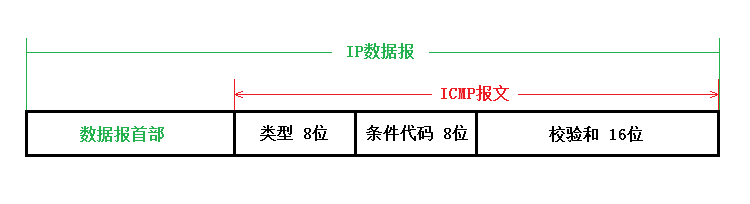
某些设备，比如无盘机在启动时可能不知道自己的 IP 地址，它们可以将自己的 MAC 地址使用 RARP 请求广播出去，RARP 服务器就会响应并回复无盘机的 IP 地址。

RARP 在目前的应用中已极少被使用，不再赘述了。

## 三、ICMP(Internet Control Message Protocol)控制报文协议

通信过程中的发生各种问题时，ICMP 将问题反馈，通过这些信息，管理者可以对所发生的问题作出诊断，然后采取适当的措施去解决它。

ICMP 报文由 8 位错误类型、8 位条件代码和 16 位校验和组成，被封装在一个 IP 数据报中：



报文的类型字段可以有 15 个不同的值，以便描述特定类型的 ICMP 报文，代码字段的值进一步描述不同的条件，各类型的报文及其处理方法如图所示：



也有一些出现差错而不产生 ICMP 报文的情况：

1.ICMP 差错报文

2 . 目的地址是广播或多播地址

3.作为链路层广播的数据报

4.不是 IP 分片的第一片

5.源地址不是单个主机的数据报（源不能为零地址、环回地址、广播多播地址）

## 四、ping 程序和 traceroute 程序

ping 程序和 traceroute 程序是两个常见的 **基于 ICMP 协议** 的工具。

**ping**

ping 程序是对两台主机之间连通性进行测试的基本工具，它只是利用 ICMP 回显请求和回显应答报文，而不用经过传输层（TCP/UDP）。

ping 程序通过在 ICMP 报文数据中存放发送请求的时间值来计算往返时间，当应答返回时，用当前时间减去存放在 ICMP 报文中的时间值，即是往返时间。

ping 程序使用方法为 **ping IP 地址** ，ping 命令还可以加上参数，实现更多的功能：

* -n 只输出数值。
* -q 不显示任何传送封包的信息，只显示最后的结果。
* -r 忽略普通的 Routing Table，直接将数据包送到远端主机上。通常是查看本机的网络接口是否有问题。
* -R 记录路由过程。
* -v 详细显示指令的执行过程。
* -c 数目：在发送指定数目的包后停止。
* -i 秒数：设定间隔几秒送一个网络封包给一台机器，预设值是一秒送一次。
* -t 存活数值：设置存活数值 TTL 的大小。

**traceroute**

traceroute 程序是用来侦测主机到目的主机之间所经路由情况的重要工具。刚才 ping 程序中讲过，带 -R 参数的 ping 命令也可以记录路由过程，但是，因为 IP 数据报头的长度限制(最多能保存 9 个 IP 地址)，ping 不能完全的记录下所经过的路由器，traceroute 正好就填补了这个缺憾。

实验楼环境没有 traceroute 程序，需要使用以下命令安装：

sudo apt-get install traceroute

traceroute 程序的工作原理很简单：

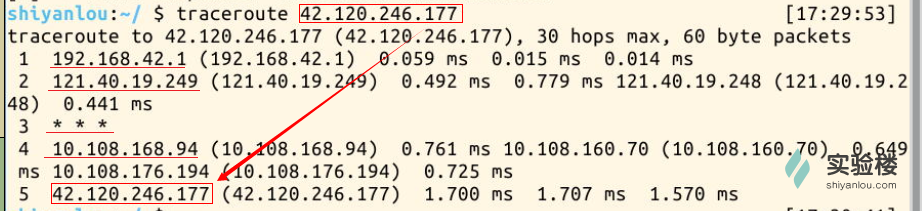
它发送一份 TTL 为 1 的 IP 数据报给目的主机，经过第一个路由器时，TTL 值被减为 0，则第一个路由器丢弃该数据报，并返回一份超时 ICMP 报文，于此得到了路径中第一个路由器的地址；

然后再发送一份 TTL 值为 2 的数据报，便可得到第二个路由器的地址；

-以此类推，一直到到达目的主机为止，这样便记录下了路径上所有的路由 IP。

**由于实验楼网络限制，下述示例可能无法执行，建议使用**traceroute git.shiyanlou.com**进行测试。**

例子：我们尝试记录到 42.120.246.177 的路由过程，可见经过 5 步最终可以到达：



## 五、IGMP(Internet Group Management Protocol)组管理协议

IGMP 是用于管理多播组成员的一种协议，它的作用在于，让其他所有需要知道自己处于哪个多播组的主机和路由器知道自己的状态。只要某一个多播组还有一台主机，多播路由器就会把数据传输出去，这样，接受方就会通过网卡过滤功能来得到自己想要的数据。 为了知道多播组的信息，多播路由器需要定时的发送 IGMP 查询，各个多播组里面的主机要根据查询来回复自己的状态。路由器来决定有几个多播组，自己要对某一个多播组发送什么样的数据。

## 六、作业

1、查看 ARP 缓存，并截图。

2、使用带选项的 ping 命令记录到git.shiyanlou.com途径的路由，并与 traceroute 命令的结果做比较。截图。