

## 一、为主机申请 IP：DHCP 动态主机配置协议

我需要一个 IP 地址，告诉网络我是谁。这就需要 DHCP 动态主机配置协议。

- 1) 主机生成一个 DHCP 请求报文（应用层）
- 2) 放入 UDP 报文段（传输层），UDP 报文段主要包含

源端口 68（DHCP 客户端的固定端口）

目的端口 67（DHCP 服务器的固定端口）

- 3) 网络层添加头部封装成 IP 数据报，主要包含

源 IP：0.0.0.0

目的 IP：255.255.255.255（广播 IP）

- 4) 数据链路层添加头部封装成以太网帧，主要包含

源 MAC：自己的 MAC

目的 MAC：FF:FF:FF:FF:FF:FF（广播帧）

- 5) 以太网帧被发送到交换机\*（他是怎么找到交换机的呢？你的网线连着呢呀），交换机修改转发表记录我的 MAC（自学习：每接收到一个帧都记录该帧的 MAC 和到达的接口），然后在他的所有出口广播这个帧

- 6) 与交换机相连的默认网关路由器接收到了这个广播帧，进行解析，提取出 IP 数据报，发现目的 IP 是广播 IP，就交给传输层，传输层又提取出 DHCP 请求交给应用层，DHCP 服务器就收到了该 DHCP 请求。

（路由器？服务器？这里路由器怎么就成服务器了呢？其实路由器的路由功能只是它众多功能的一种，他还可以支持别的协议，比如这里的 DHCP 协议）

- 7) DHCP 服务器为此生成一个 DHCP ACK 报文，主要包含：

分配给 DHCP 请求的 IP

DNS 服务器的 IP

默认网关路由器的 IP

子网掩码

这个报文再被传输层、网络层、数据链路层一路封装成帧，该帧的目的 MAC 是我的 MAC，源 MAC 是接收 DHCP 请求帧的路由器端口的 MAC

- 8) DHCP ACK 以太网帧由默认网关路由器发送给交换机，交换机根据转发表转发回给我的主机

- 9) 主机收到该帧之后再从链路层到应用层，层层提取，最后得到自己的 IP、DNS 服务器 IP、默认网关路由器 IP，进行配置，我就有了 IP。

## 二、查找默认网关路由器的 MAC 地址：ARP 地址转换协议

现在我有了源 IP，要开始找目的 IP，现在我已知什么呢？已知目的域名，根据域名找 IP，找 DNS 域名系统服务器去查就好。在前面 DHCP 过程中我们已经得到了 DNS 服务器的 IP 地址，现在只要去访问该 IP 就好，但是在这之前我们需要先走出我们所处的局域网，这就需要局域网默认网关路由器的 MAC 地址，这是为什么呢？又要怎么找呢？继续往下看。

先解释一下默认网关路由器，每一个主机都在一个局域网里，要访问局域网以外的主机就需要先离开这个局域网，那我们要怎么离开呢？我们把这个局域网比作一个院子，网关路由器就是这个院子的门，我们要离开这个院子的话就要从门出去，那一个院子可以有很多个门，我们从哪个门出去呢？我们自己也不知道啊，但一般都有一个默认的，不知道该从哪出去的时候，就走默认的。

为什么需要局域网的 MAC 地址呢？因为局域网内是通过 MAC 进行识别的，为什么要用 MAC 地址识别呢？是这样的，以前没这么多主机的时候，IP 是固定的，我们就不需要 MAC，但现在主机越来越多，这就导致局域网里 IP 不是十分充足，管理起来也不是很好管理，所以 IP 每隔一段

时间就会被回收，需要的时候才会被分配，这也就是为什么前面提到的 DHCP 动态主机配置协议会存在，所以这个 IP 是会变的，对于主机来说，唯一不变的是 MAC，所以，在局域网内部我们是用 MAC 定位的。

那又要怎么找 MAC 地址呢？通过 IP 找 MAC，这就用到了 ARP 地址转换协议。

10) 主机生成一个 ARP 查询报文，目的 IP 是默认网关路由器，这个报文最终被封装成以太网帧，帧的目的 MAC 是 FF:FF:FF:FF:FF:FF (广播地址)，然后把帧发给交换机，交换机看到是广播地址就给广播出去

11) 默认网关路由器接收到了这个帧，经过层层提取得到 ARP 报文，发现其中的目的 IP 跟他自己某个接口的 IP 匹配，就发送回去一个 ARP 应答报文给主机，这里包含他自己的 MAC

### 三、查找目的域名的 IP：DNS 域名系统

现在我们拿到了默认网关路由器的 MAC，可以离开局域网去 DNS 服务器查目的域名的 IP 了

12) 主机生成 DNS 查询报文，包含

目的域名

DNS 服务器目的端口：53

层层封装成以太网帧，帧的目的 MAC 是默认网关路由器的 MAC

13) 默认网关路由器接收到该帧之后，提取出 IP 数据报，并根据路由表进行转发，因为路由器具有内部网关协议\* (RIP 路由信息协议、OSPF 开放最短路径优先协议) 和外部网关协议 (BGP 边界网关协议)\*，因此路由表中已经配置了可以从路由器到达 DNS 服务器的路由表项

14) DNS 服务器接收到帧后，层层提取出 DNS 查询报文，并在 DNS 数据库中查找待解析域名对应的 IP，找到之后发送 DNS 应答报文，封装成 UDP 报文段，再放入 IP 数据报，最后通过路由器转回给源主机的默认网关路由器，再经由交换机转发给源主机。

### 四、TCP 三次握手

这样我就拿到了目的域名的 IP，就可以进行 TCP 的三次握手了。

15) (第一次握手) 主机向目的服务器发送连接请求报文段，SYN=1，ACK=0，选择一个初始的序号  $x_0$ 。

16) (第二次握手) 目的服务器收到连接请求报文段后，如果同意建立连接，则向主机发送连接确认报文段，SYN=1，ACK=1，确认号为  $x+1$ ，同时也选择一个初始的序号  $y_0$ 。

17) (第三次握手) 主机收到目的服务器的连接确认报文段后，还要向目的服务器发出确认，确认号为  $y+1$ ，序号为  $x+1$ 。

18) 目的服务器收到主机的确认后，连接就建立了。

为什么要进行第三次握手呢？

第三次握手是为了防止失效的连接请求到达服务器，让服务器错误打开连接。

客户端发送的连接请求如果在网络中滞留，那么就会隔很长一段时间才能收到服务器端发回的连接确认。客户端等待一个超时重传时间之后，就会重新请求连接。但是这个滞留的连接请求最后还是会到达服务器，如果不进行三次握手，那么服务器就会打开两个连接。如果有第三次握手，客户端会忽略服务器之后发送的对滞留连接请求的连接确认，不进行第三次握手，因此就不会再次打开连接。

19) 连接建立完成了，现在我们可以继续前言中连接建立之后的过程进行访问了