今天我们正式来到了应用层，第一个我们先来看下DHCP协议。

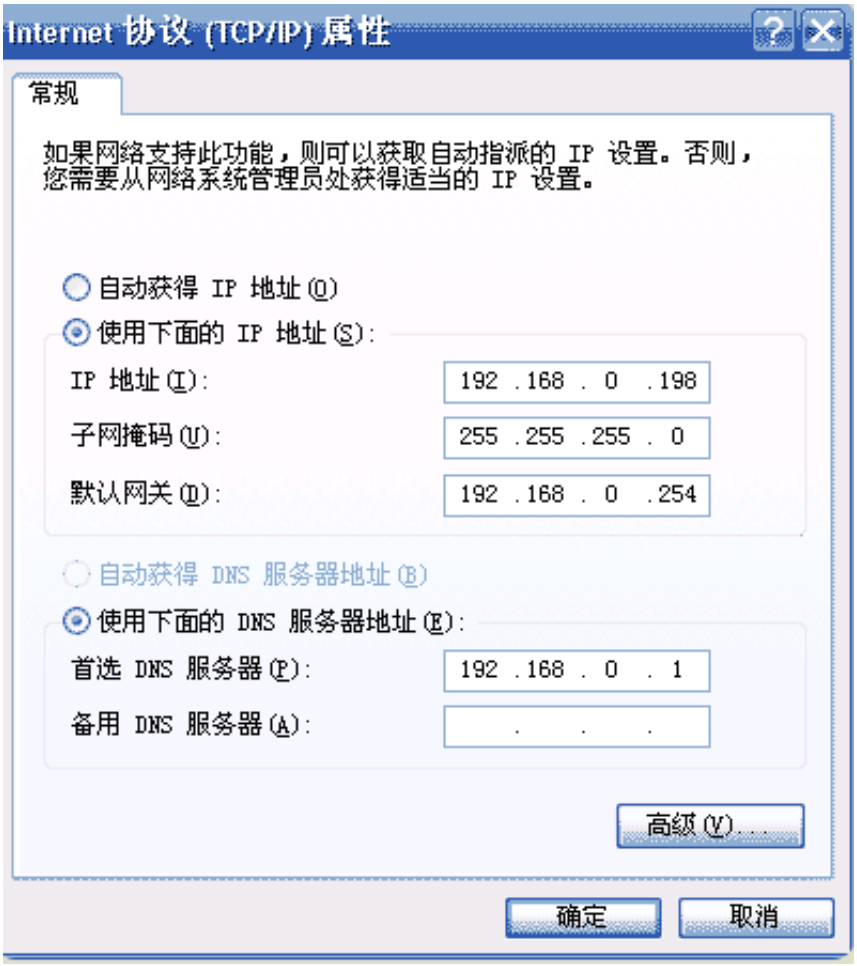
我们知道IP地址极其重要，IP地址分为公网IP地址和内网IP地址，前者是花钱申请的，数量有限；后者是免费的，仅用于内网使用。那么内网中，我们电脑的IP地址是如何获取的呢?

首先，我们要知道，获取IP的方式有两种：

- **手动的**（manual）：或者称为静态的（static），你可以自己选择机器的 IP 地址。
- **动态的**（dynamic）：IP 地址由服务器提供。这个服务器被称为 DHCP 服务器，实际上DHCP 服务器除了 IP 地址的分配以外还有其他用途。

一、DHCP有什么用

让我们先来看下手动配置的方式，我们进入一家公司，这个公司可能为你的工位分配了一个静态IP，并且会给你提供一些参数进行连接。有可能是这样的：



这让普通用户望而生畏，我们需要填写网关的地址、子网掩码以及DNS服务器的地址，如果有一个填错了，那么可能就无法访问互联网，不过更大的问题在于可能会引发冲突，因为网络中有很多的机器，很有可能就与另外一台机器配置的IP重复了。

因此，我们会意识到，**使用一种快速可靠的机制来为网络上的机器分配 IP 地址是很必要的**，接下来舞台留给 DHCP 。

二、DHCP原理

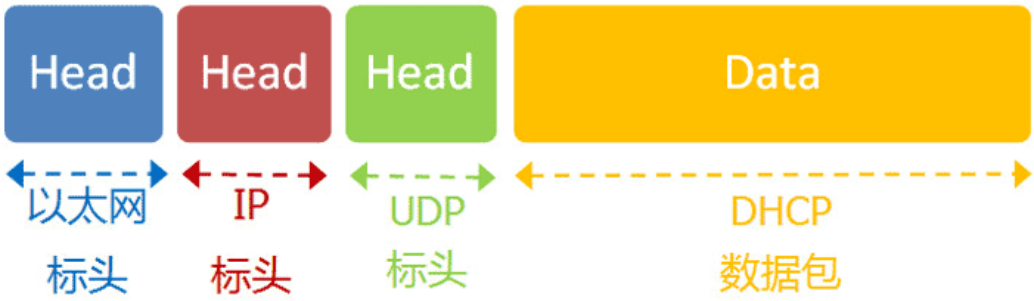
DHCP 是 Dynamic Host Configuration Protocol 的缩写，表示 **“动态主机配置协议”** 。

所谓"动态"，指计算机开机后，会自动分配到一个IP地址，不用人为设定。

这个协议规定，每一个子网络中，有一台计算机负责管理本网络的所有IP地址，它叫做"DHCP服务器"。既然是统一分配，自然也就不会出现冲突的情况。新的计算机加入网络，必须向"DHCP服务器"发送一个"DHCP请求"数据包，申请IP地址和相关的网络参数。

前面说过，如果两台计算机在同一个子网络，必须知道对方的MAC地址和IP地址，才能发送数据包。但是，新加入的计算机不知道DHCP服务器的两个地址，怎么发送数据包呢?

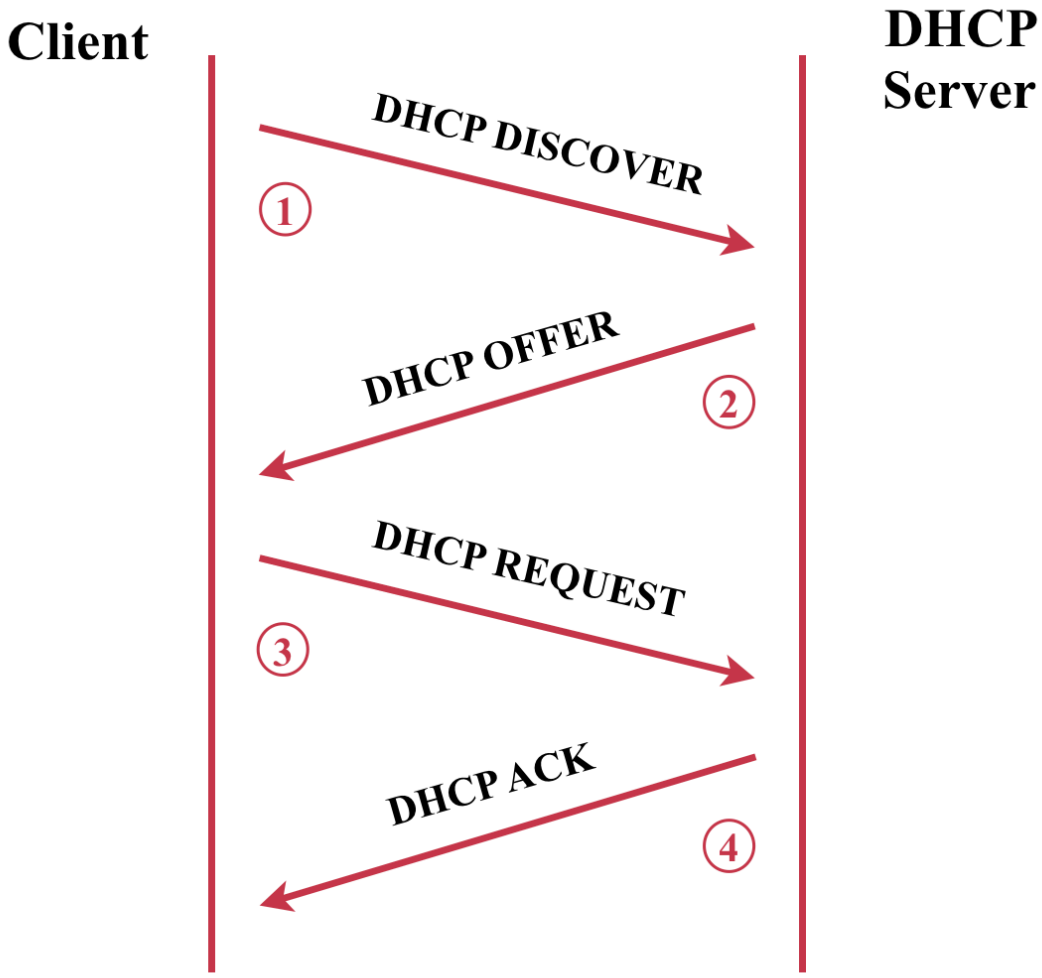
首先，**DHCP协议是一种应用层协议，建立在UDP协议之上**，所以整个数据包是这样的：



假设我们就是需要获取IP等参数的机器。**我们只知道自己的 mac 地址，其他啥都不知道，这个时候，如何跟 DHCP 服务器通信呢?**

答案自然就是广播，在局域网内，广播的用途还是挺多的，比如之前提过的 ARP 协议。

大致流程如图所示：



具体流程如下：

DHCP 协议采用 UDP 协议作为第 4 层（传输层）的协议，**客户端发送请求消息到 DHCP 服务器的 67 号端口，DHCP 服务器发送回应消息给客户端的 68 号端口**。

- ①客户端发送一个 **DHCP DISCOVER 帧**，目的MAC地址填的是 `ff:ff:ff:ff:ff:ff`，因此同一网络内的所有机器都会收到这个广播帧。
- ②我们的 DHCP 服务器收到 DHCP DISCOVER 帧，它将发送回一个提议，这是一个 **DHCP OFFER 帧**。它将提供一个 IP 地址，子网掩码，以及默认网关的 IP 地址，有时还提供 DNS 服务器的 IP 地址。
- ③当我们客户端接受了上一步返回的信息，会以 **DHCP REQUEST 帧**来响应，这个帧也是以广播形式发送，用于告知接受了哪个提议（offer）。
- ④提议已被接受的 DHCP 服务器将确认请求，并发送 **DHCP ACK 帧**，以确认“租约”（lease）的分配。

注意，我们提到了**租约**这个词语，说明 IP 地址的分配是有期限的，过了期限之后，必须重新请求一个 IP 地址。

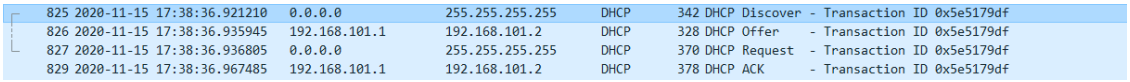
不过，要续订“租约”（重新请求一个 IP 地址）时，客户端不需要进行从 DHCP DISCOVER 开始的整个过程，而是直接从 DHCP REQUEST 开始。DHCP 服务器会把与 MAC 地址关联的已分配的 IP 地址保存在内存中。因此，即使你的“租约”确实已续签多次，你有时仍会保留相同的 IP 地址很长时间。

三、通过抓包验证

家里有宽带网络的，可以直接实验。

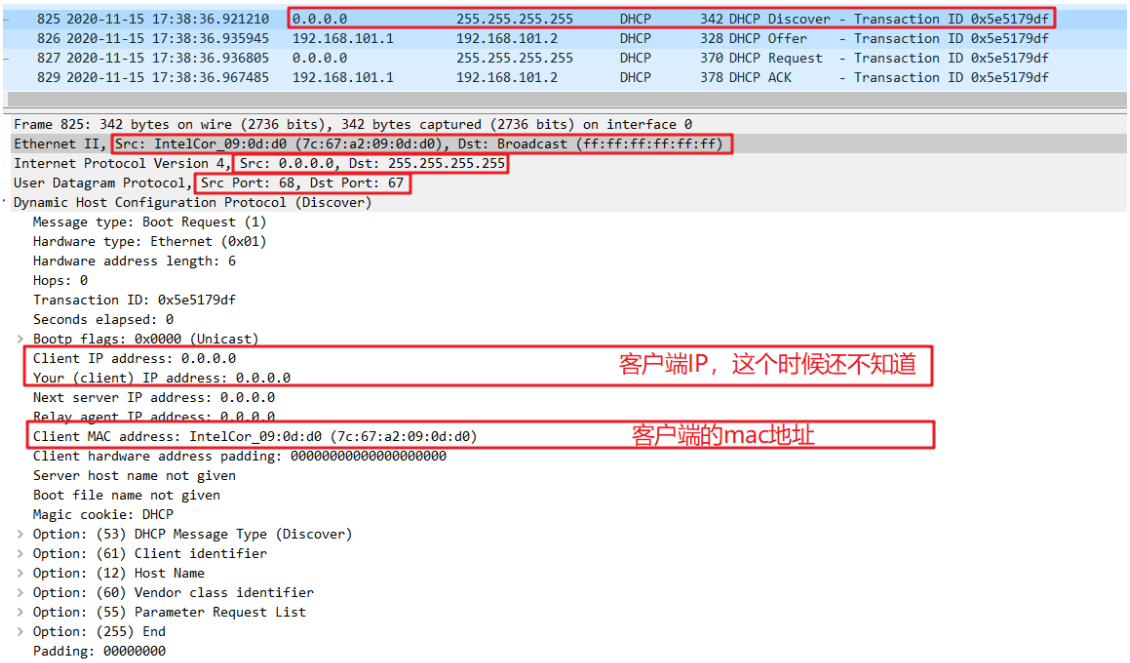
本地打开 wireshark 进行抓包，首先在 cmd 中输入：ipconfig /release ，清空所有匹配连接。然后使用 ipconfig /renew 更新所有连接。

> wireshark的抓包教程马上就要奉上，不要着急，由于软件使用起来很简单，读者朋友可以自行安装并尝试抓包试试，比如抓取下ping百度的包。



可以看到，renew 指令的抓包正好对应了上述的四个过程。我们一个个来看下报文。

①首先是 DHCP DISCOVER 帧，请求 DHCP 服务器分配 ip 信息：



②然后 DHCP 服务器返回 DHCP OFFER 帧，本地路由器（图中可以看到是192.168.101.1）充当了 DHCP 的角色为我们分配了一个内网ip和子网掩码信息返回给我们，我们可以看到为我们分配了192.168.101.2：

```
  825 2020-11-15 17:38:36.921210   0.0.0.0          255.255.255.255    DHCP     342 DHCP Discover - Transaction ID 0x5e5179df
  826 2020-11-15 17:38:36.935945   192.168.101.1    192.168.101.2      DHCP     328 DHCP Offer    - Transaction ID 0x5e5179df
  827 2020-11-15 17:38:36.936805   0.0.0.0          255.255.255.255    DHCP     370 DHCP Request  - Transaction ID 0x5e5179df
  829 2020-11-15 17:38:36.967485   192.168.101.1    192.168.101.2      DHCP     378 DHCP ACK      - Transaction ID 0x5e5179df

> Frame 826: 328 bytes on wire (2624 bits), 328 bytes captured (2624 bits) on interface 0
> Ethernet II, Src: 4c:50:77:a0:49:98 (4c:50:77:a0:49:98), Dst: IntelCor_09:0d:d0 (7c:67:a2:09:0d:d0)
> Internet Protocol Version 4, Src: 192.168.101.1, Dst: 192.168.101.2
> User Datagram Protocol, Src Port: 67, Dst Port: 68
v Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x5e5179df
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.101.2          为我们分配的ip地址是这个
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: IntelCor_09:0d:d0 (7c:67:a2:09:0d:d0)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Offer)           表示是一个offer报文
  > Option: (54) DHCP Server Identifier (192.168.101.1)
  > Option: (51) IP Address Lease Time
  > Option: (58) Renewal Time Value
  > Option: (59) Rebinding Time Value
  > Option: (1) Subnet Mask (255.255.255.0)          子网掩码信息
  > Option: (3) Router
  > Option: (6) Domain Name Server
  > Option: (255) End
```

我们看下本地内网IP地址：

```
无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::9d96:deb3:3989:9411%22
   IPv4 地址 . . . . . . . . . . . . : 192.168.101.2
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.101.1

C:\Users\swg>
```

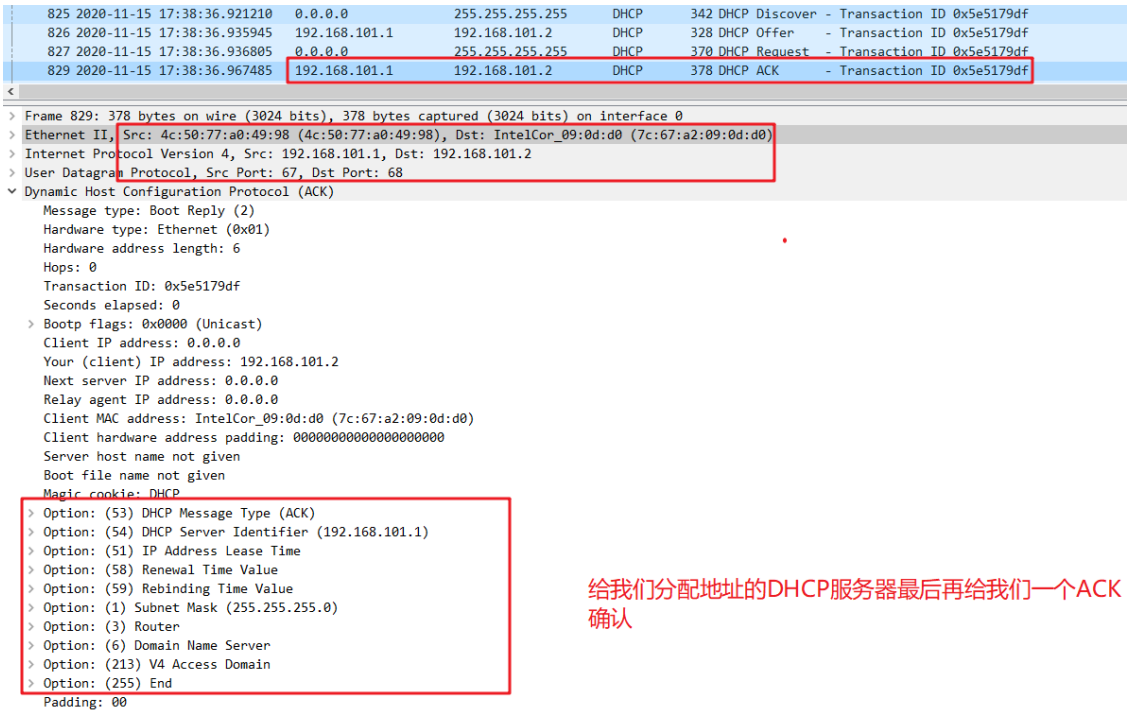
③客户端再次发出广播信息 DHCP REQUEST 帧，告诉所有 DHCP 服务器我接受了谁的提议：

```
  825 2020-11-15 17:38:36.921210   0.0.0.0          255.255.255.255    DHCP     342 DHCP Discover - Transaction ID 0x5e5179df
  826 2020-11-15 17:38:36.935945   192.168.101.1    192.168.101.2      DHCP     328 DHCP Offer    - Transaction ID 0x5e5179df
  827 2020-11-15 17:38:36.936805   0.0.0.0          255.255.255.255    DHCP     370 DHCP Request  - Transaction ID 0x5e5179df
  829 2020-11-15 17:38:36.967485   192.168.101.1    192.168.101.2      DHCP     378 DHCP ACK      - Transaction ID 0x5e5179df

> Frame 827: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface 0
> Ethernet II, Src: IntelCor_09:0d:d0 (7c:67:a2:09:0d:d0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)   客户端又发出了一个广播帧
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x5e5179df
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: IntelCor_09:0d:d0 (7c:67:a2:09:0d:d0)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Request)
  > Option: (61) Client identifier
  > Option: (50) Requested IP Address (192.168.101.2)
  > Option: (54) DHCP Server Identifier (192.168.101.1)
  > Option: (12) Host Name
  > Option: (81) Client Fully Qualified Domain Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
  > Option: (255) End
```

将分配到的信息也广播出去，让其他的DHCP服务器也可以知道

④被接受提议的 DHCP 服务器确认这个广播信息，返回 DHCP ACK 确认分配。



给我们分配地址的DHCP服务器最后再给我们一个ACK确认

整体过程总结为表格为：

阶段	源MAC	目标MAC	源IP	目标IP
DHCP DISCOVER	客户机的MAC	广播地址，全FF	0.0.0.0	255.255.255.255
DHCP OFFER	DHCP服务器或者中继器路由的MAC	客户机的MAC	DHCP服务器或者中继路由器的IP地址	准备分配的IP地址
DHCP REQUEST	客户机的MAC	广播地址，全FF	0.0.0.0	255.255.255.255
DHCP ACK	DHCP服务器或者中继器路由的MAC	客户机的MAC	DHCP服务器或者中继路由器的IP地址	准备分配的IP地址

通过实验，也可以发现，我们的路由器为我们默默做了这么多事情，谢谢你，路由器！谢谢你，DHCP协议！不禁要为你们歌唱：

> 听我说谢谢你
> 因为有你 温暖了四季
> 谢谢你 感谢有你
> 世界更美丽