[**wait\_for\_y**](https://www.cnblogs.com/kwaitfort/)

[Wireshark分析DHCP](https://www.cnblogs.com/kwaitfort/p/9104457.html)

文章转载  自  <https://blog.csdn.net/qq_24421591/article/details/50936469>

**（0.0.0.0已经不是一个真正意义上的IP地址了。 　　它表示的是这样一个集合：**

**1、所有不清楚的主机和目的网络。这里的“不清楚”是指在本机的路由表里没有特定条目指明如何到达。**

**2、对本机来说，它就是一个“收容所”，所有不认识的“三无”人员，一 律送进去。）**

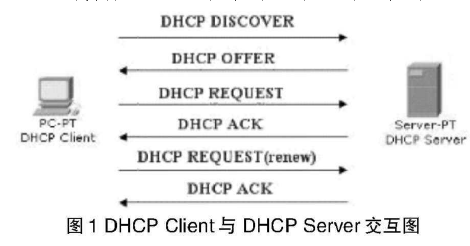
**一，动态主机配置协议DHCP**

**1,DHCP简介**

DHCP(Dynamic Host Configuration Protocol),动态主机配置协议，是一个应用层协议。当我们将客户主机ip地址设置为动态获取方式时，DHCP服务器就会根据DHCP协议给客户端分配IP，使得客户机能够利用这个IP上网。

DHCP的前身是BOOTP协议（Bootstrap Protocol）,BOOTP被创建出来为连接到网络中的设备自动分配地址，后来被DHCP取代了，DHCP比BOOTP更加复杂，功能更强大。后面可以看到，在用Wireshark过滤显示DHCP包，需要输入过滤条件BOOTP，而不是DHCP,但或许是因为我使用的Wireshark版本是比较旧的1.12.9,没有在新版本中尝试过，也许可以输入DHCP让其只显示DHCP包。

**2，DHCP的实现**

  
DHCP的实现分为4步，分别是：  
第一步：Client端在局域网内发起一个DHCP　Discover包，目的是想发现能够给它提供IP的DHCP Server。  
第二步：可用的DHCP Server接收到Discover包之后，通过发送DHCP Offer包给予Client端应答，意在告诉Client端它可以提供IP地址。  
第三步：Client端接收到Offer包之后，发送DHCP Request包请求分配IP。  
第四步：DHCP Server发送ACK数据包，确认信息。

**二，利用Wireshark抓取DHCP包**

**1,分析**

要想抓取到DHCP包，先要保证有可用的DHCP服务器，然后将主机IP地址获取方式设置为自动获取。如果主机在抓包之前已经联网，需要先断开主机的网络连接，然后再连接网络。在cmd下使用命令ipconfig来完成网络断开与连接的过程：

ipconfig /release 断开主机当前的网络连接

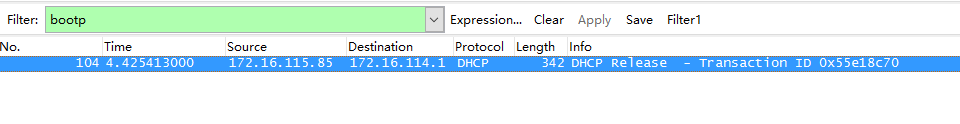
ipconfig /renew 请求连接网络

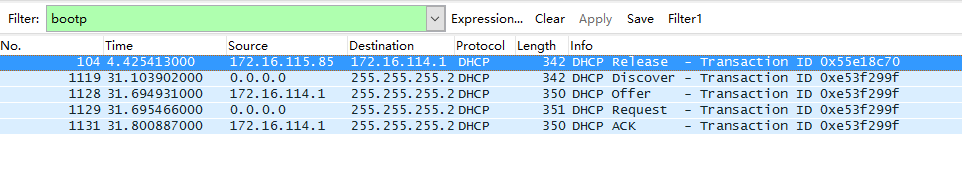
* 1
* 2
* 3

在cmd中可以使用ipconfig /?查看各参数的含义：  
  
(1)ipconfig /release  
断开当前的网络连接，主机IP变为0.0.0.0，主机与网络断开，不能访问网络。  
(2)ipconfig /renew  
更新适配器信息，请求连接网络，这条命令结束之后，主机会获得一个可用的IP，再次接入网络。

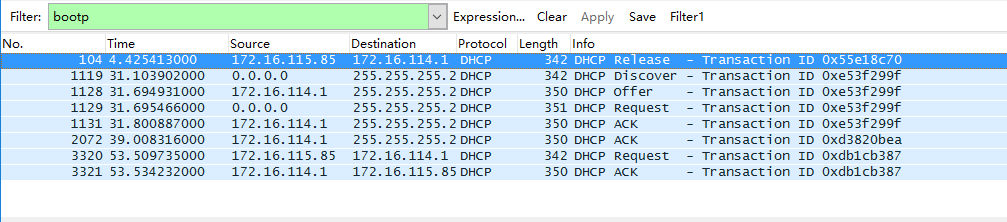
**2,开始抓包**

实验环境：Win10,Wireshark1.12.9，有线连接  
(1)在Wireshark中点击start开始抓包，在过滤栏输入bootp，使其只显示DHCP数据包。  
(2)在cmd中输入ipconfig /release 断开网络连接。  
  
可以看到此时所有的网卡都已经断开。以太网处于断开状态。

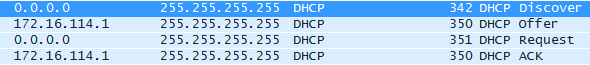
  
Wireshark中截获到一个DHCP Release数据包。

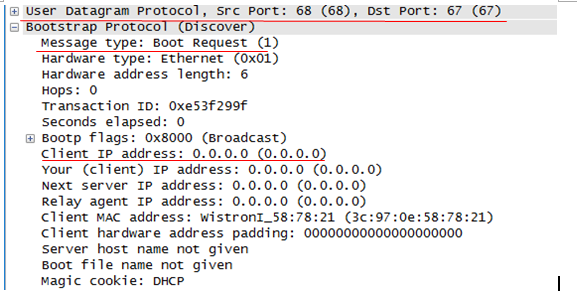
(3)在cmd中输入ipconfig /renew 请求网络连接。  
  
此时，可以看到在Wireshark中新增了4个DHCP数据包：  
数据包1：**DHCP Discover**  
数据包2：**DHCP Offer**  
数据包3：**DHCP Request**  
数据包4：**DHCP ACK**

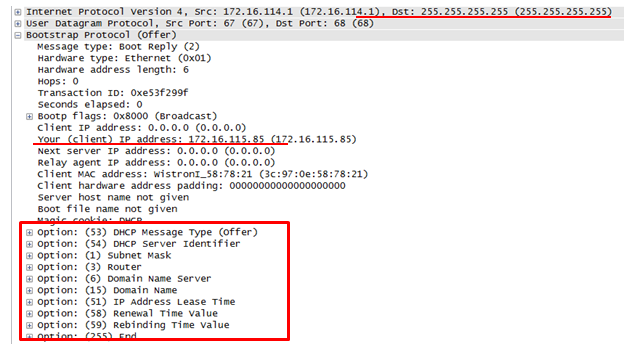
  
等待这条命令执行完毕之后，在cmd中可以看到主机被分配了IP，主机成功连入网络中。

(4)为了后续分析使用，我们再执行一次ipconfig /renew：  
  
可以看到Wireshark中新增了3个数据包：DHCP ACK；DHCP Request;DHCP ACk。  
如果再次使用ipconfig /renew,每执行一次会新增2个数据包：DHCP Request;DHCP ACk。

**三，DHCP包分析**

下面着重来分析当执行，ipconfig /renew这条命令产生的4个DHCP数据包，这4个数据包代表了客户机和DHCP服务器的交互过程，也是IP动态分配的过程。  
  
**1，DHCP Discover数据包**  
(1)Client端使用IP地址0.0.0.0发送了一个广播包，可以看到此时的目的IP为255.255.255.255。Client想通过这个数据包发现可以给它提供服务的DHCP服务器。

(2)从下图可以看出，DHCP属于应用层协议，它在传输层使用UDP协议，目的端口是67。  


**2，DHCP Offer包**  
当DHCP服务器收到一条DHCP Discover数据包时，用一个DHCP Offerr包给予客户端响应。  
  
(1)DHCP服务器仍然使用广播地址作为目的地址，因为此时请求分配IP的Client并没有自己ip,而可能有多个Client在使用0.0.0.0这个IP作为源IP向DHCP服务器发出IP分配请求，DHCP也不能使用0.0.0.0这个IP作为目的IP地址，于是依然采用广播的方式，告诉正在请求的Client们，这是一台可以使用的DHCP服务器。

(2)DHCP服务器提供了一个可用的IP,在数据包的Your (client) IP Address字段可以看到DHCP服务器提供的可用IP。

(3)除此之外，如图中红色矩形框的内容所示，服务器还发送了子网掩码，路由器，DNS，域名，IP地址租用期等信息。

**3，DHCP Request包**  
当Client收到了DHCP Offer包以后（如果有多个可用的DHCP服务器，那么可能会收到多个DHCP Offer包），确认有可以和它交互的DHCP服务器存在，于是Client发送Request数据包，请求分配IP。  
此时的源IP和目的IP依然是0.0.0.0和255.255.255.255。

**4，DHCP ACK包**  
服务器用DHCP ACK包对DHCP请求进行响应。  
