

# DHCP协议详解（非常详细总结），结合ENSP,wireshark学习使用

原创 JIANXIN.Y 发布于2019-04-20 13:07:56 阅读数 859 ☆ 收藏

## 1 DHCP协议

### 1.1 DHCP协议理解

**定义：**DHCP：Dynamic Host Configuration Protocol，动态主机配置协议，是一个应用在局域网中的网络协议，它使用UDP协议工作。

**理解：**DHCP协议就是一个基于UDP协议工作在局域网内的网络协议，其最终的目的就是获取响应的IP地址，其中这过程中有多种分配以及发送请求等。

**作用：**动态分配IP地址，过程自动化，终端无需——手工配置，配置信息统一管理（DNS,网关），IP地址有限、需要大量配置IP地址、移动终端。

**好处：**提高配置IP地址效率，减少配置工作量，减少IP地址冲突。

#### 分配IP地址方式：

- （1）**手工配置方式：**通过网络管理员手工配置某台客户端特定的IP地址，当客户端请求分配时，DHCP服务器就将手动配置的IP地址分配给客户端。。
- （2）**自动配置方式：**当DHCP客户端第一次想服务端租用到第一个IP地址后，就将这个IP地址永久分配给客户端使用。
- （3）**动态配置方式：**服务器暂时分配一个IP地址给客户端，根据租约到期或者续约租期的方式来管理分配的IP地址。

### 1.2 DHCP报文格式

链路层头	IP头 20bytes	UDP头	DHCP报文
------	-------------	------	--------

图1 DHCP报文封装格式



图2 DHCP报文格式

图1是dhcp整个报文的封装格式，包括链路层头、IP头、UDP头和DHCP报文，其中dhcp主要的数据都封装在dhcp报文中。

图2 就是DHCP报文的格式，各字段的说明如下：

- op：**1byte,是报文的操作类型，分为请求报文和响应报文，1为请求报文；2为响应报文。具体的报文类型在option字段中标识。
- htype：**1byte,表示client硬件地址的类型，1表示以太网类型。
- hlen：**1byte，硬件地址的长度，以太网的硬件地址长度为6bytes。
- hops：**1byte，表示当前dhcp报文经过的DHCP中继的数目，每经过一个DHCP中继这个字段就加1。
- xid：**4bytes，由client端产生的随机数，用于匹配请求和应答报文，就是匹配应答报文是对哪个请求报文做出应答。
- secs：**2bytes，客户端进入IP地址申请进程的时间或者更新IP地址进程的时间；由客户端软件根据情况设定。目前没有使用，固定为0。
- flags：**2bytes，是标志字段，16比特中只使用了最高位比特（即最左边的比特），这个个比特是广播响应标识位，用来标识DHCP服务器发出的响应：是单播，0是单播，1是广播。其余的比特位保留不用，都为0。

**ciaddr:** 4bytes，是客户端的IP地址，可以是client自己的IP地址，也可以是server分配给client的IP地址。

**yiaddr**(Your IP Address): 4bytes，是server分配给client的IP地址。

**siaddr:** 4bytes，是client端获取IP地址等信息的server端的地址。

**giaddr:** 4bytes，是client发出请求报文后经过的第一个中继的IP地址。

**chaddr:** 16bytes，是client端的**硬件地址**，在client发出报文时会把自己网卡的硬件地址写进这个字段。

**sname:** 64bytes，服务器主机名，是client端获取IP地址等信息的服务器名称。

**file:** 128bytes，是client的启动配置文件名，是服务器为client指定的启动配置文件名及路径信息，由服务器填写。

**options:** 是可选变长的选项字段，这个字段包含了终端的初始配置信息和网络配置信息，包括报文类型，有效租期，DNS服务器的IP地址等。这个字段的结构采用“CLV”结构，如图4：

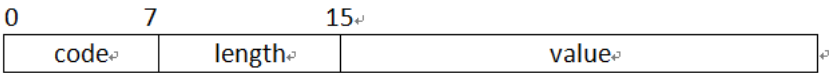


图4 option字段编码方式

其中“code”是标识号，唯一标识后面的信息内容(vlaue),1bytes;

“length”表示后面的value值的长度，1bytes

“vlaue”是信息内容

Options字段有很多项，是可选的，不同的报文option项可能不同，图5是一个DHCP request报文的option项：

- ▷ Option: (53) DHCP Message Type (Request)
- ▷ Option: (61) Client identifier
- ▷ Option: (50) Requested IP Address
- ▷ Option: (12) Host Name
- ▷ Option: (81) Client Fully Qualified Domain Name
- ▷ Option: (60) Vendor class identifier
- ▷ Option: (55) Parameter Request List
- ▷ Option: (255) End

图5 option项

不同的option项有不同的含义，下面是一些常见的option项：

- (1) DHCP Message Type: code=53 length=1 表示DHCP的报文类型。
- (2) Client identifier: code=61 client端的硬件地址
- (3) Server identifier: code=54 服务器的IP地址
- (4) Subnet Mask: code=1 子网掩码
- (5) route: code=3 网关IP地址
- (6) Domain Name Server: code=6 DNS服务器的IP地址
- (7) IP Address Lease Time: code=51 租约时间

### 1.3 DHCP协议报文的种类

Dhcp协议一共有8中报文，包括：DHCPDISCOVERY, DHCPPOFFER, DHCPREQUEST, DHCPACK, DHCPNAK, DHCPRELEASE, DHCPDECLIN, DHCPINFORM。

报文类型由options字段中的option53 “DHCP Message Type”选项来确定。各报文的具体含义如下：

- (1) , **DHCP-DISCOVER**报文: 0x01 **客户端请求包**

这个报文是client端开始dhcp过程的第一个请求报文，client在请求地址时，并不知道server端的位置，所以client会以广播的方式发送请求报文，它的网络中的服务器。

(2) , **DHCP-OFFER**报文: 0x02 **服务器响应包**

这个报文server端对DISCOVERY报文的响应报文。会在所配置的地址池中查找一个合适的IP地址，加上相应的租约期限和其他配置信息（如网关、DNS SERVER等），构造一个OFFER报文，发送给用户，告知用户本SERVER可以为其提供IP地址的分配，并且。发OFFER报文一般是单播的。

(3) , **DHCP-REQUEST**报文: 0x03 **客户端选择包**

在一个子网中可能有多台服务器，所有收到DISCOVER报文的服务器都会回应OFFER报文，所以client端可能收到多个OFFER报文，通过选择第一个服务器作为自己的目标服务器，并回应一个REQUEST请求报文。在续租约的时候client端也会发送REQUEST报文 请求续租期。

(4) , **DHCP-ACK**报文: 0x05 **服务器确认包**

是server对client端的REQUEST报文的确认响应报文，server在收到REQUEST报文后，根据REQUEST报文中携带的client MAC来查找是否有则发送ACK报文作为回应，通知client可以使用分配的IP地址。

(5) , **DHCP-NAK**报文: 0x06 **服务器拒绝包**

Server端对client端的REQUEST报文的拒绝响应报文，如果服务器没有相应的租约记录，就会发送NAK报文给client端。

(6) , **DHCP-RELEASE**报文: 0x07 **客户端释放包**

Client端主动释放server端分配给它的IP是，就会发送DHCP-RELEASE报文给server，server收到这个报文后，就会回收这个IP地址。

(7) , **DHCP-DECLINE**报文: 0x04

client收到server回应的ACK报文后，通过地址冲突检测发现 SERVER分配的地址冲突或由于其它原因导致不能使用，则发送DHCP-DECLINE报文，通知分配的IP地址不可用。

(8) , **DHCP-INFORM**报文: 0x08

在client已经获得了IP地址，需要从server端获得更详细的配置信息时，就会发送DHCP-INFORM报文向server请求，server在收到这个报文后，会根据找到相应的配置信息后，就会回应DHCP-ACK报文给client。

## 1.4 DHCP协议工作过程

### 1.4.1 动态获取IP过程

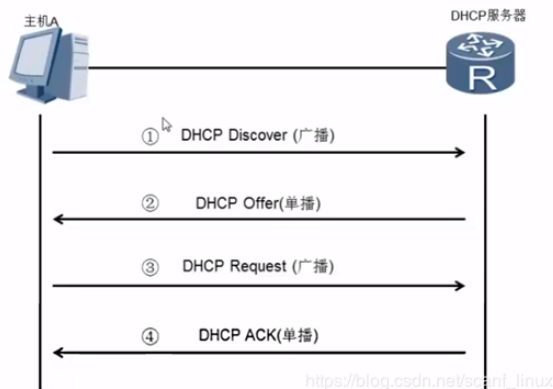


图5 DHCP工作流程

#### 1.2.1.1 抓包过程

- (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win10 中的cmd输入ipconfig /release 先断开当前的网络连接，主机号变为0.0.0.0，主机与网络断开，不能访问网络。

```
C:\Users\Unionman>ipconfig /release
```

```
以太网适配器 以太网:
    连接特定的 DNS 后缀 . . . . . :
    本地连接 IPv6 地址. . . . . : fe80::5cad:1328:ac7b:e1d2%7
    默认网关. . . . . : fe80::1%7
```

图6 断开网络配置图

No.	Time	Source	Destination	Protocol	Length	Info
1732	28.287670	192.168.100.2	192.168.100.1	DHCP	342	DHCP Release - Transaction ID 0xf1279f1

图7 释放包

(3) 在cmd中输入ipconfig /renew 请求网络连接，也为客户端分配了IP地址。

```
C:\Users\Unionman>ipconfig /renew
```

```
以太网适配器 以太网:
    连接特定的 DNS 后缀 . . . . . :
    本地连接 IPv6 地址. . . . . : fe80::5cad:1328:ac7b:e1d2%7
    IPv4 地址 . . . . . : 192.168.100.2
    子网掩码 . . . . . : 255.255.255.0
    默认网关. . . . . : fe80::1%7
                        192.168.100.1
```

图8 再次请求网络配置图

Source	Destination	Protocol	Length	Info
192.168.100.2	192.168.100.1	DHCP	342	DHCP Release - Transaction ID 0xf1279f1
0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xce80fc10
192.168.100.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0xce80fc10
0.0.0.0	255.255.255.255	DHCP	357	DHCP Request - Transaction ID 0xce80fc10
192.168.100.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0xce80fc10

图9 新增数据包

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

1.4.1.2 DHCP四个阶段

DHCP动态获取IP地址的过程主要分为发现阶段、提供阶段、选择阶段、确认阶段四个阶段。

(1)发现阶段：client端在局域网内以广播的方式发起一个DHCP Discover包，目的是在子网络中发现能够给client端提供IP地址的server端。

UDP 目标端口号为67 源IP 地址0.0.0.0 目的IP:255.255.255.255

```
> Frame 9: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: LcfcHefe_21:c5:03 (50:7b:9d:21:c5:03), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
* Bootstrap Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xb11b528d
  Seconds elapsed: 0
  > Bootstrap 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: LcfcHefe_21:c5:03 (50:7b:9d:21:c5:03)
```

图10 DHCP discover包

(2)提供阶段：局域网中DHCP server接受到Discover包之后，通过发送DHCP offer包给client端应答，主要是告知client端可以提供IP地址，以及相应信息和其他配置信息也会在其中。

UDP 目标68 源IP为DHCP服务器的IP 目的IP:255.255.255.255

```
Ethernet II, Src: Epigram_32:33:41 (00:90:4c:32:33:41), Dst: LcfcHefe_21:c5:03 (50:7b:9d:21:c5:03)
Internet Protocol Version 4, Src: 192.168.88.254, Dst: 192.168.88.100
User Datagram Protocol, Src Port: 67 (67), Dst Port: 68 (68)
Bootstrap Protocol (Offer)
  Message type: Boot Reply (2)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xb1b528d
  Seconds elapsed: 0
  Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 192.168.88.100
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: LcfcHefe_21:c5:03 (50:7b:9d:21:c5:03)
```

```
Option: (53) DHCP Message Type (Offer)
  Length: 1
  DHCP: Offer (2)
Option: (54) DHCP Server Identifier
  Length: 4
  DHCP Server Identifier: 192.168.88.254
Option: (51) IP Address Lease Time
  Length: 4
  IP Address Lease Time: (86400s) 1 day
Option: (1) Subnet Mask
  Length: 4
  Subnet Mask: 255.255.255.0
Option: (3) Router
  Length: 4
  Router: 192.168.88.254
Option: (6) Domain Name Server
  Length: 4
  Domain Name Server: 192.168.88.254
Option: (255) End
```

租约

子网掩码

网关

DNS

图11 DHCP offer包

(3)选择阶段：在client端可能会接受到多个offer包，通常clientdaunt只会接受收到的第一个DHCP offer报文，然后client端就会以广播的方式发送一request报文请求分配IP地址。

UDP 目标67 源IP为0.0.0.0 目的IP:255.255.255.255

```
Ethernet II, Src: LcfcHefe_21:c5:03 (50:7b:9d:21:c5:03), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
Bootstrap Protocol (Request)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xcfc332221
  Seconds elapsed: 0
  Bootp flags: 0x8000, Broadcast flag (Broadcast)
  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: LcfcHefe_21:c5:03 (50:7b:9d:21:c5:03)
```

```
Option: (53) DHCP Message Type (Request)
Option: (61) Client identifier
Option: (50) Requested IP Address
  Length: 4
  Requested IP Address: 192.168.88.100
Option: (54) DHCP Server Identifier
  Length: 4
  DHCP Server Identifier: 192.168.88.254
Option: (12) Host Name
Option: (81) Client Fully Qualified Domain Name
Option: (60) Vendor class identifier
Option: (55) Parameter Request List
Option: (255) End
```

请求的IP

服务器的IP

图12 DHCP REQUEST包

(4)确认阶段：server端在收到DHCP request报文之后，会判断“option”字段的serverIP地址是否是自己的IP地址，如果符合分配IP地址的条件，就送一个DHCP ACK包，如果不满足就发送一个DHCP NAK包。

UDP 目标68 源IP为DHCP服务器的IP 目的IP:255.255.255.255

```
Ethernet II, Src: Epigram_32:33:41 (00:90:4c:32:33:41), Dst: LcfcHefe_21:c5:03 (50:7b:9d:21:c5:03)
Internet Protocol Version 4, Src: 192.168.88.254, Dst: 192.168.88.100
User Datagram Protocol, Src Port: 67 (67), Dst Port: 68 (68)
Bootstrap Protocol (ACK)
  Message type: Boot Reply (2)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xb1b528d
  Seconds elapsed: 0
  Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 192.168.88.100
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: LcfcHefe_21:c5:03 (50:7b:9d:21:c5:03)
```

ACK报文  
单播的方式发送

```
Ethernet II, Src: Epigram_32:33:41 (00:90:4c:32:33:41), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.88.254, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 67 (67), Dst Port: 68 (68)
Bootstrap Protocol (NAK)
  Message type: Boot Reply (2)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xe7da1d6
  Seconds elapsed: 0
  Bootp flags: 0x8000, Broadcast flag (Broadcast)
  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: LcfcHefe_21:c5:03 (50:7b:9d:21:c5:03)
```

NAK拒绝响应报文  
拒绝分配IP给client  
广播发送

图13 DHCP ACK 包

注意：客户端执行DHCP-DISCOVER后，如果没有DHCP服务器响应客户端的请求，客户端会随机使用169.254.0.0/16网段中的一个...地址配置到本169.254.0.0/16是Windows的自动私有IP寻址范围，也就是在无法通过DHCP获取IP地址时，由系统自动分配的IP地址段。



### 1.4.2 续约租期

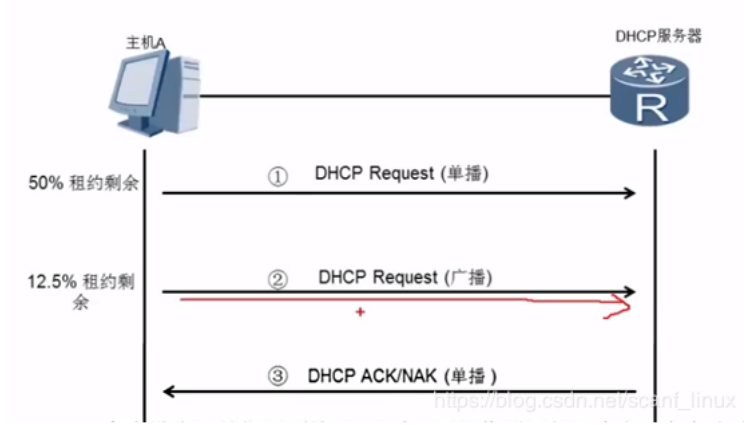


图14 续约租期过程

- (1) 当clientIP地址已经用到50%的时间，续租一下，client端就会以单播形式向服务端发送一个DHCP Request包，当server响应时，应一个AC约定一个时间。

(2) 当clientIP地址已经用到50%的时间，续租一下，client端就会以单播形式向服务端发送一个DHCP Request包，server没有响应，client会继续用到87.5%时，会在续租一次，同时就以广播的方式是发送一个request包，server这时收到响应以后，就会回应一个ACK包，重新约定一个时间。

(3) 当clientIP地址已经用到50%的时间，续租一下，client端就会以单播形式向服务端发送一个DHCP Request包，server没有响应，client会继续用到87.5%时，会在续租一次，同时就以广播的方式是发送一个request包，如果server还是没有响应，client那就直接使用到过期。

### 1.4.3 重新连接使用IP地址

Client端在重新登录网络的时候，可以不需要从初始阶段发送DHCP DISCOVER报文开始，可以直接广播发送DHCP REQUEST报文给服务器。

Option: (53) DHCP Message Type (Request)

Option: (61) Client identifier

Length: 7

Hardware type: Ethernet (0x01)

Client MAC address: LcfcHefe\_21:c5:03 (50:7b:9d:21:c5:03)

Option: (50) Requested IP Address

Length: 4

Requested IP Address: 192.168.222.108

Option: (12) Host Name

Option: (81) Client Fully Qualified Domain Name

Option: (60) Vendor class identifier

Option: (55) Parameter Request List

Option: (255) End

### 1.4.4 client主动释放IP地址

Frame 1732: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0

Ethernet II, Src: HewlettP\_e3:f0:8d (40:b0:34:e3:f0:8d), Dst: ChinaMob\_4c:07:a0 (c0:d0:ff:4c:07:a0)

Internet Protocol Version 4, Src: 192.168.100.2, Dst: 192.168.100.1

User Datagram Protocol, Src Port: 68, Dst Port: 67

Bootstrap Protocol (Release)

Message type: Boot Request (1)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0x0f1279f1

Seconds elapsed: 0

Bootp flags: 0x0000 (Unicast)

Client IP address: 192.168.100.2

图16 DHCP release报文