

DHCP 报文格式

dhcp 有 8 种类型的报文，每种报文的格式相同，只是报文中的某些字段取值不同。dhcp 报文格式基于 bootp（引导程序协议）的报文格式，具体格式如图 1-2 所示（括号中的数字表示该字段所占的字节）：客户端采用 UDP 端口号：68；服务器采用 UDP 端口号：67

op(1)	htype(1)	hlen(1)	hops(1)
xid(4)			
secs(2)		flags(2)	
ciaddr(4)			
yiaddr(4)			
siaddr(4)			
giaddr(4)			
chaddr(16)			
sname(64)			
file(128)			
option(variable)			

图1-2 DHCP报文格式

各字段的解释如下：

op: dhcp 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。

htype、hlen: dhcp 客户端的硬件地址类型及长度。

hops: dhcp 报文经过的 dhcp 中继的数目。dhcp 请求报文每经过一个 dhcp 中继，该字段就会增加 1。

xid: 客户端发起一次请求时选择的随机数，用来标识一次地址请求过程。

secs: dhcp 客户端开始 dhcp 请求后的时间。

flags: 第一个比特为广播响应标识位，用来标识 dhcp 服务器响应报文是采用单播还是广播发送。其余比特保留不用。

ciaddr: dhcp 客户端的 ip 地址。

yiaddr: dhcp 服务器分配给客户端的 ip 地址。

siaddr: dhcp 客户端获取 ip 地址等信息的服务器 ip 地址。

giaddr: dhcp 客户端发出请求报文后经过的第一个 dhcp 中继的 ip 地址。

chaddr: dhcp 客户端的硬件地址。

sname: dhcp 客户端获取 ip 地址等信息的服务器名称。

file: dhcp 服务器为 dhcp 客户端指定的启动配置文件名称。

option: 可选变长选项字段, 包含报文的类型、有效租期、dns (domain name system, 域名系统) 服务器的 ip 地址、wins 服务器的 ip 地址等配置信息。

BOOTP 报文格式:



下面是抓到的一个完整的 DHCP 请求过程：

1、DHCP discover 报文 不知道 DHCP server 地址用广播

No. .	Time	Source	Destination	Protocol	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID: 0x2c8a0740
Frame 1 (511 bytes) on wire (511 bytes captured)					
Ethernet II, Src: 02:00:4c:4f:4f:50 (02:00:4c:4f:4f:50), Dst: Broadcast (ff:ff:ff:ff:ff:ff)					
Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)					
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)					
Bootstrap Protocol					
Message type: Boot Request (1)					
Hardware type: Ethernet					
Hardware address length: 6					
Hops: 0					
Transaction ID: 0x2c8a0740					
Seconds elapsed: 0					
Bootp flags: 0x0000 (Unicast)					
Client IP address: 0.0.0.0 (0.0.0.0)					
Your (client) IP address: 0.0.0.0 (0.0.0.0)					
Next server IP address: 0.0.0.0 (0.0.0.0)					
Relay agent IP address: 0.0.0.0 (0.0.0.0)					
Client MAC address: 02:00:4c:4f:4f:50 (02:00:4c:4f:4f:50)					
Server host name not given					
Boot file name not given					
Magic cookie: (OK)					
Option 53: DHCP Message Type = DHCP Discover					
Option 116: DHCP Auto-Configuration (1 bytes)					
Option 61: Client identifier					
Option 50: Requested IP Address = 192.168.3.5 主机以前的静态IP地址					
Option 12: Host Name = "liqingru-7c71e8"					
Option 60: Vendor class identifier = "MSFT 5.0"					
Option 55: Parameter Request List					
End Option					

2、DHCP offer 报文 cisco 用单播来实现

No. .	Time	Source	Destination	Protocol	Info
2	0.081589	192.168.2.2	192.168.2.1	DHCP	DHCP Offer - Transaction ID: 0x2c8a0740
Frame 2 (511 bytes) on wire (511 bytes captured)					
Ethernet II, Src: ca:00:05:50:00:00 (ca:00:05:50:00:00), Dst: 02:00:4c:4f:4f:50 (02:00:4c:4f:4f:50)					
Internet Protocol, Src: 192.168.2.2 (192.168.2.2), Dst: 192.168.2.1 (192.168.2.1)					
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)					
Bootstrap Protocol					
Message type: Boot Reply (2)					
Hardware type: Ethernet					
Hardware address length: 6					
Hops: 0					
Transaction ID: 0x2c8a0740					
Seconds elapsed: 0					
Bootp flags: 0x0000 (Unicast)					
Client IP address: 0.0.0.0 (0.0.0.0)					
Your (client) IP address: 192.168.2.1 (192.168.2.1)					
Next server IP address: 0.0.0.0 (0.0.0.0)					
Relay agent IP address: 0.0.0.0 (0.0.0.0)					
Client MAC address: 02:00:4c:4f:4f:50 (02:00:4c:4f:4f:50)					
Server host name not given					
Boot file name not given					
Magic cookie: (OK)					
Option 53: DHCP Message Type = DHCP offer					
Option 54: Server Identifier = 192.168.2.2					
Option 51: IP Address Lease Time = 23 hours, 55 minutes, 45 seconds					
Option 58: Renewal Time Value = 11 hours, 57 minutes, 52 seconds					
Option 59: Rebinding Time value = 20 hours, 56 minutes, 16 seconds					
Option 1: Subnet Mask = 255.255.255.0					
Option 3: Router = 192.168.2.2					
End option					

3、DHCP request 报文 客户端还没有 IP 地址用广播

No.	Time	Source	Destination	Protocol	Info
3	0.081941	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction
Frame 3 (368 bytes on wire, 368 bytes captured)					
Ethernet II, Src: 02:00:4c:4f:4f:50 (02:00:4c:4f:4f:50), Dst: Broadcast (ff:ff:ff:ff:ff:ff)					
Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)					
Version: 4					
Header length: 20 bytes					
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)					
0000 00.. = Differentiated Services Codepoint: Default (0x00)					
.... ..0. = ECN-Capable Transport (ECT): 0					
.... ...0 = ECN-CE: 0					
Total Length: 354					
Identification: 0x1e94 (7828)					
Flags: 0x00					
0... = Reserved bit: Not set					
.0.. = Don't fragment: Not set					
..0. = More fragments: Not set					
Fragment offset: 0					
Time to live: 128					
Protocol: UDP (0x11)					
Header checksum: 0x1af8 [correct]					
Source: 0.0.0.0 (0.0.0.0)					
Destination: 255.255.255.255 (255.255.255.255)					
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)					
Bootstrap Protocol					
Message type: Boot Request (1)					
Hardware type: Ethernet					
Hardware address length: 6					
Hops: 0					
Transaction ID: 0x2c8a0740					
Seconds elapsed: 0					
Bootp flags: 0x0000 (Unicast)					
Client IP address: 0.0.0.0 (0.0.0.0)					
Your (client) IP address: 0.0.0.0 (0.0.0.0)					
Next server IP address: 0.0.0.0 (0.0.0.0)					
Relay agent IP address: 0.0.0.0 (0.0.0.0)					
Client MAC address: 02:00:4c:4f:4f:50 (02:00:4c:4f:4f:50)					
Server host name not given					
Boot file name not given					
Magic cookie: (OK)					
Option 53: DHCP Message Type = DHCP Request					
Option 61: Client identifier					
Option 50: Requested IP Address = 192.168.2.1					
Option 54: Server Identifier = 192.168.2.2					
Option 12: Host Name = "liqingru-7c71e8"					
Option 81: FQDN					
Option 60: Vendor class identifier = "MSFT 5.0"					
Option 55: Parameter Request List					
End option					

4、DHCP ack 报文 cisco 用得也是单播

No. .	Time	Source	Destination	Protocol	Info
4	0.143596	192.168.2.2	192.168.2.1	DHCP	DHCP ACK - Transaction
<div> <div> Ethernet II, Src: ca:00:05:50:00:00 (ca:00:05:50:00:00), Dst: 02:00:4c:4f:4f:50 (02:00:4c:4f:4f:50) </div> <div> Internet Protocol, Src: 192.168.2.2 (192.168.2.2), Dst: 192.168.2.1 (192.168.2.1) </div> <div> User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68) </div> <div> <div>Bootstrap Protocol</div> <div> <div>Message type: Boot Reply (2)</div> <div>Hardware type: Ethernet</div> <div>Hardware address length: 6</div> <div>Hops: 0</div> <div>Transaction ID: 0x2c8a0740</div> <div>Seconds elapsed: 0</div> <div>Bootp flags: 0x0000 (Unicast)</div> <div>Client IP address: 0.0.0.0 (0.0.0.0)</div> <div>Your (client) IP address: 192.168.2.1 (192.168.2.1)</div> <div>Next server IP address: 0.0.0.0 (0.0.0.0)</div> <div>Relay agent IP address: 0.0.0.0 (0.0.0.0)</div> <div>Client MAC address: 02:00:4c:4f:4f:50 (02:00:4c:4f:4f:50)</div> <div>Server host name not given</div> <div>Boot file name not given</div> <div>Magic cookie: (OK)</div> <div>Option 53: DHCP Message Type = DHCP ACK</div> <div>Option 54: Server Identifier = 192.168.2.2</div> <div>Option 51: IP Address Lease Time = 1 day</div> <div>Option 58: Renewal Time Value = 12 hours</div> <div>Option 59: Rebinding Time Value = 21 hours</div> <div>Option 1: Subnet Mask = 255.255.255.0</div> <div>Option 3: Router = 192.168.2.2</div> <div>End Option</div> </div> </div> </div>					

在整个请求过程中，Transaction ID 不改变，代表一次请求过程。

我用的是 DynamipsGUI 模拟的 cisco 7200 路由器做的 DHCP 服务器