

MINH HOẠ PHÂN TÍCH GÓI TIN GIAO THỨC DHCP

I. Mục Tiêu:

Bài hướng dẫn này giúp sinh viên có thể:

- Nhắc lại cơ chế hoạt động của giao thức DHCP
- Sử dụng công cụ wireshark để bắt gói tin và phân tích hoạt động của một giao thức

II. Nội dung

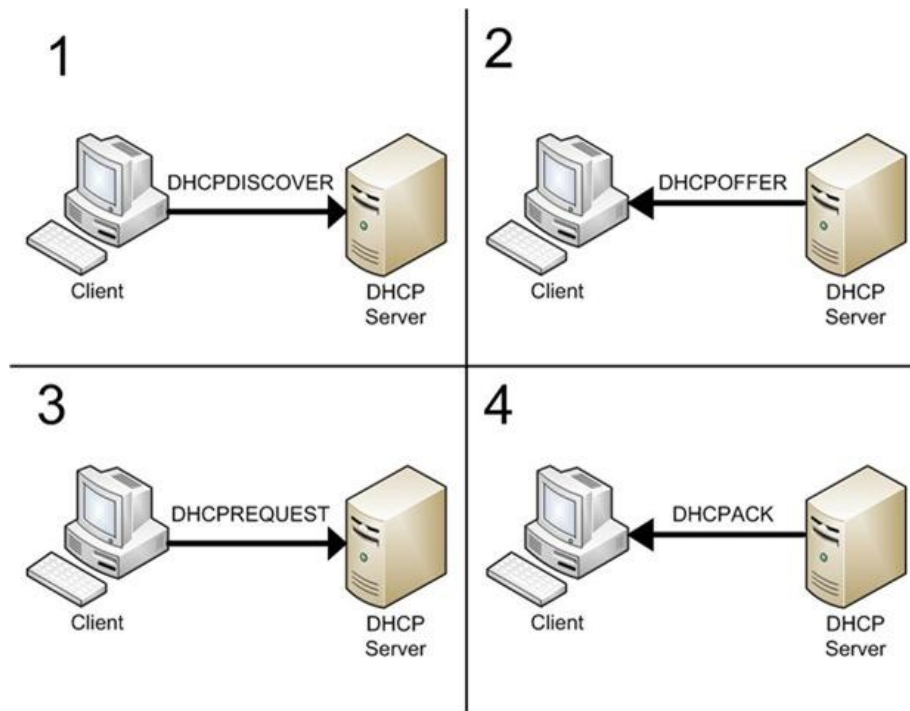
II.1. Nhắc lại DHCP

Dynamic Host Configuration Protocol (DHCP) là một giao thức hoạt động ở tầng ứng dụng, cho phép cấu hình địa chỉ IP của các máy trạm một cách tự động. Từ đó có thể quản lý tập trung địa chỉ IP của các máy trong một mạng nội bộ hạn chế được xung đột có thể xảy ra cũng như dễ dàng cập nhật các thay đổi có thể có về địa chỉ IP của công ty.

DHCP hoạt động như một phần mở rộng của giao thức BOOTP. Ngoài việc cung cấp khả năng cấu hình IP cho các máy con, DHCP còn cho phép người quản trị thiết lập các trường khác như DNS server hay WINS server.

II.2. Cơ chế hoạt động

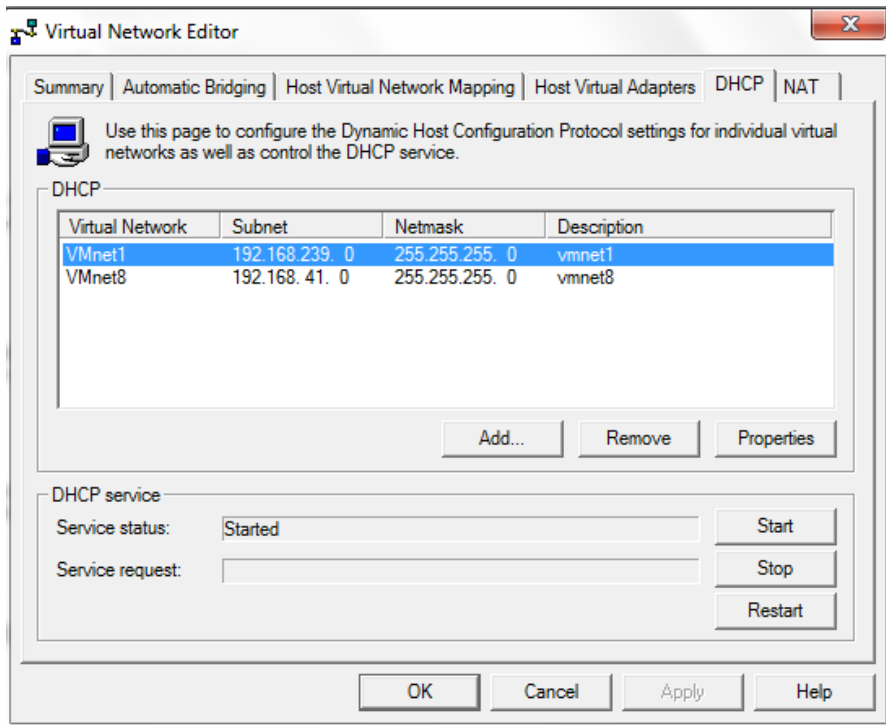
Quá trình hoạt động của giao thức DHCP được mô tả gồm 4 bước sau đây :



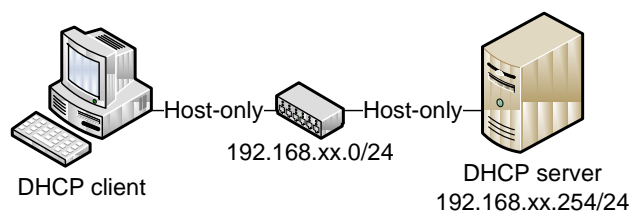
II.3. Chuẩn bị :

Tắt dịch vụ DHCP trong chương trình VMware

Chọn menu Edit → Virtual Network Setting. Trong cửa sổ Virtual Network Editor, chọn tab DHCP (hình bên dưới) → chọn card mạng tương ứng → chọn Stop → chọn Apply



Tạo một mạng gồm 2 máy ảo theo mô hình



Máy Server:

- Hệ điều hành: Windows 2003 Server
- IP: 192.168.1.1/24
- Cài đặt dịch vụ DHCP server và cấu hình cấp phát địa chỉ cho một lớp mạng 192.168.1.0/24, khoảng cấp phát nằm trong khoảng từ 192.168.1.10/24 - 192.168.1.100/24 theo mô hình sau với xx = 0

Máy Client:

- IP: nhận IP động
- Cài đặt chương trình Wireshark

II.4. Tiến hành bắt gói tin trên máy client theo các bước sau :

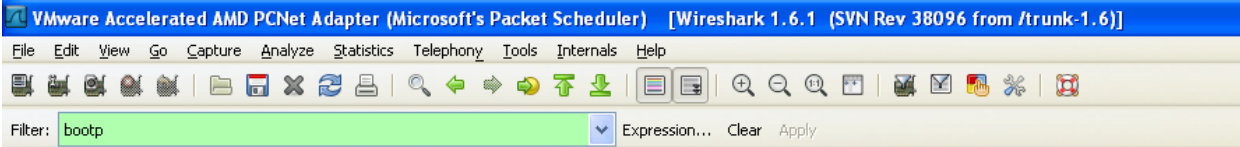
1. Mở cửa sổ Windows Command Prompt (Start → Run → cmd) và gõ lệnh “*ipconfig /release*”.
2. Khởi động quá trình bắt gói tin của Wireshark.
3. Quay lại cửa sổ Windows Command Prompt gõ lệnh “*ipconfig /renew*”.
4. Đợi đến khi lệnh “*ipconfig /renew*” kết thúc, gõ lệnh “*ipconfig /renew*” một lần nữa.
5. Đợi đến khi lệnh “*ipconfig /renew*” thứ hai kết thúc, gõ lệnh “*ipconfig /release*” một lần nữa.
6. Cuối cùng, thực hiện lại lệnh “*ipconfig /renew*” lần thứ ba.
7. Kết thúc quá trình bắt gói tin của Wireshark.

II.5. Phân tích quá trình hoạt động của DHCP

Sử dụng Wireshark để bắt các gói tin theo các bước trên, ta sẽ thu được rất nhiều các gói tin thuộc các giao thức khác nhau, không chỉ là các gói tin của DHCP. Vì mỗi khi máy nhận được một địa chỉ IP mới, nó thường phát sinh kèm theo đó các gói tin để thông báo cho các máy khác sự tồn tại của mình trong mạng.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xef9b2257
2	0.001855	192.168.1.254	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xef9b2257
3	0.002113	0.0.0.0	255.255.255.255	DHCP	368	DHCP Request - Transaction ID 0xef9b2257
4	0.003288	192.168.1.254	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xef9b2257
5	0.012829	Vmware_5b:ef:6a	Broadcast	ARP	42	Gratuitous ARP for 192.168.1.10 (Request)
6	0.348945	Vmware_5b:ef:6a	Broadcast	ARP	42	Gratuitous ARP for 192.168.1.10 (Request)
7	1.348912	Vmware_5b:ef:6a	Broadcast	ARP	42	Gratuitous ARP for 192.168.1.10 (Request)
8	2.374077	192.168.1.10	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
9	2.382620	192.168.1.10	224.0.0.22	IGMP	54	v3 Membership Report / Join group 239.255.255.250 for any sources
10	2.399941	192.168.1.10	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
11	2.427369	192.168.1.10	192.168.1.255	NBNS	110	Registration NB TIENTRAN-DAE24A<00>
12	3.176989	192.168.1.10	192.168.1.255	NBNS	110	Registration NB TIENTRAN-DAE24A<00>
13	3.349024	192.168.1.10	224.0.0.22	IGMP	54	v3 Membership Report / Join group 239.255.255.250 for any sources
14	3.926917	192.168.1.10	192.168.1.255	NBNS	110	Registration NB TIENTRAN-DAE24A<00>
15	4.118689	192.168.1.10	192.168.1.254	DHCP	356	DHCP Request - Transaction ID 0xc2863620
16	4.119238	192.168.1.254	192.168.1.10	DHCP	342	DHCP ACK - Transaction ID 0xc2863620
17	4.677051	192.168.1.10	192.168.1.255	NBNS	110	Registration NB TIENTRAN-DAE24A<00>

Ta chỉ quan tâm đến giao thức DHCP vì vậy cần phải tiến hành lọc các gói tin dạng này. DHCP sử dụng dựa trên giao thức BOOTP nên ta nhập tên giao thức này vào cửa sổ Filter.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xef9b2257
2	0.001855	192.168.1.254	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xef9b2257
3	0.002113	0.0.0.0	255.255.255.255	DHCP	368	DHCP Request - Transaction ID 0xef9b2257
4	0.003288	192.168.1.254	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xef9b2257
15	4.118689	192.168.1.10	192.168.1.254	DHCP	356	DHCP Request - Transaction ID 0xc2863620
16	4.119238	192.168.1.254	192.168.1.10	DHCP	342	DHCP ACK - Transaction ID 0xc2863620
30	10.479522	192.168.1.10	192.168.1.254	DHCP	342	DHCP Release - Transaction ID 0x5be56aa1
31	15.211450	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x11afb4ec
32	15.211901	192.168.1.254	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x11afb4ec
33	15.212107	0.0.0.0	255.255.255.255	DHCP	368	DHCP Request - Transaction ID 0x11afb4ec
34	15.212532	192.168.1.254	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x11afb4ec

Câu hỏi 1 : DHCP sử dụng giao thức nào cho tầng vận chuyển ?

Về mặt lịch sử DHCP xây dựng dựa trên giao thức BOOTP sử dụng giao thức UDP cho tầng vận chuyển. Ta có thể thấy rõ điều này khi không thấy các bắt tay ba bước của giao thức TCP trên các gói tin bắt được.

Kiểm tra với các gói tin bắt được bằng Wireshark, ta thấy ở mục Internet Protocol sử dụng UDP.

VMware Accelerated AMD PCNet Adapter (Microsoft's Packet Scheduler) [Wireshark 1.6.1 (SVN Rev 38096 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: bootp Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xef9b2257
2	0.001855	192.168.1.254	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xef9b2257
3	0.002113	0.0.0.0	255.255.255.255	DHCP	368	DHCP Request - Transaction ID 0xef9b2257
4	0.003288	192.168.1.254	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xef9b2257
15	4.118689	192.168.1.10	192.168.1.254	DHCP	356	DHCP Request - Transaction ID 0xc2863620
16	4.119238	192.168.1.254	192.168.1.10	DHCP	342	DHCP ACK - Transaction ID 0xc2863620
30	10.479522	192.168.1.10	192.168.1.254	DHCP	342	DHCP Release - Transaction ID 0x5be56aa1
31	15.211450	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x11afb4ec
32	15.211901	192.168.1.254	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x11afb4ec
33	15.212107	0.0.0.0	255.255.255.255	DHCP	368	DHCP Request - Transaction ID 0x11afb4ec
34	15.212532	192.168.1.254	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x11afb4ec

Frame 1: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits)

Ethernet II, Src: VMware_5b:ef:6a (00:0c:29:5b:ef:6a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, 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: Not-ECT (Not ECN-Capable Transport))

Total Length: 330

Identification: 0x00ec (236)

Flags: 0x00

Fragment offset: 0

Time to live: 128

Protocol: UDP (17)

Header checksum: 0x38b8 [correct]

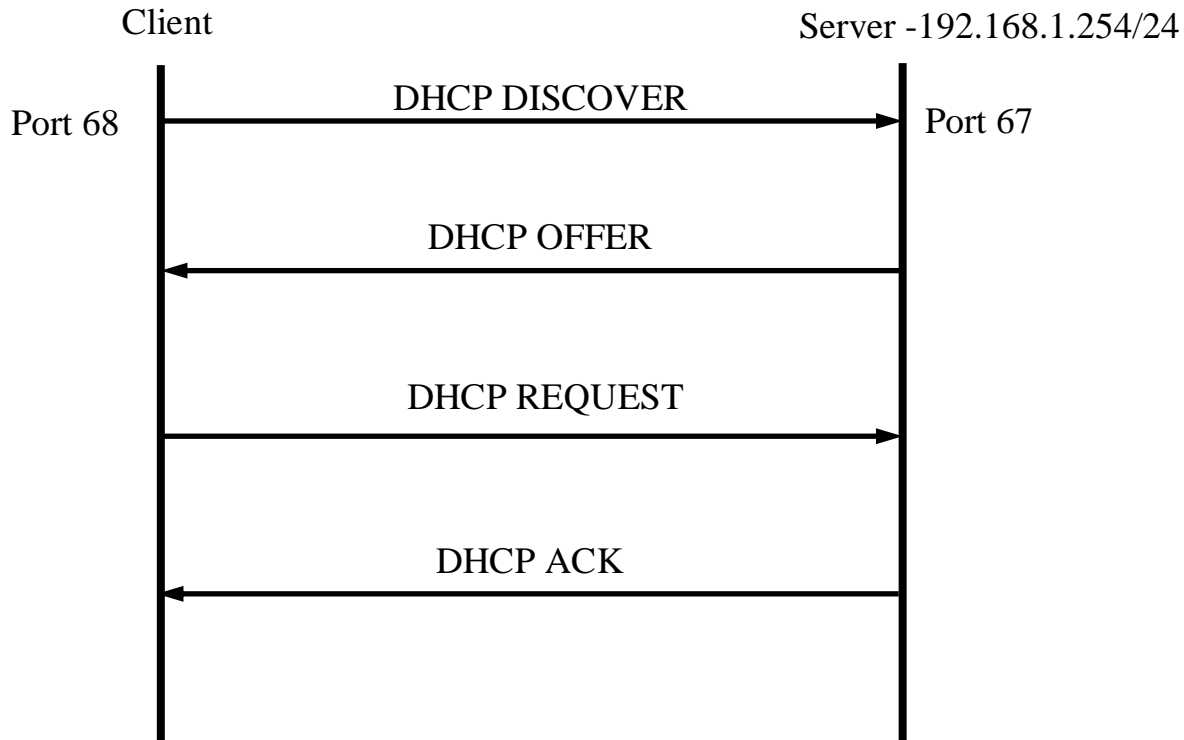
Source: 0.0.0.0 (0.0.0.0)

Destination: 255.255.255.255 (255.255.255.255)

User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)

Bootstrap Protocol

Câu hỏi 2 : Vẽ đồ thị thời gian thể hiện thứ tự của 4 gói tin DHCP :



Câu hỏi 3 : Địa chỉ ở tầng Datalink của máy Client là gì :

Ta sẽ coi địa chỉ Mac của máy client ở phần Ethernet II thu được địa chỉ sau:

MAC = 00:0c:29:5b:ef:6a

Filter: bootp						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xef9b2257
2	0.001855	192.168.1.254	255.255.255.255	DHCP	342	DHCP offer - Transaction ID 0xef9b2257
3	0.002113	0.0.0.0	255.255.255.255	DHCP	368	DHCP Request - Transaction ID 0xef9b2257
4	0.003288	192.168.1.254	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xef9b2257
15	4.118689	192.168.1.10	192.168.1.254	DHCP	356	DHCP Request - Transaction ID 0xc2863620
16	4.119238	192.168.1.254	192.168.1.10	DHCP	342	DHCP ACK - Transaction ID 0xc2863620
30	10.479522	192.168.1.10	192.168.1.254	DHCP	342	DHCP Release - Transaction ID 0x5be56aa1
31	15.211450	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x11afb4ec
32	15.211901	192.168.1.254	255.255.255.255	DHCP	342	DHCP offer - Transaction ID 0x11afb4ec
33	15.212107	0.0.0.0	255.255.255.255	DHCP	368	DHCP Request - Transaction ID 0x11afb4ec
34	15.212532	192.168.1.254	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x11afb4ec

+ Frame 1: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits)	
+ Ethernet II, Src: Vmware_5b:ef:6a (00:0c:29:5b:ef:6a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)	
+ Destination: Broadcast (ff:ff:ff:ff:ff:ff)	
+ Source: vmware_5b:ef:6a (00:0c:29:5b:ef:6a)	
Type: IP (0x0800)	
+ Internet Protocol Version 4, 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	

Câu hỏi 4 : Địa chỉ nguồn và đích của các gói tin :

DHCP DISCOVER

Source IP : 0.0.0.0

Destination IP : 255.255.255.255

DHCP OFFER

Source IP : 192.168.1.254

Destination IP : 255.255.255.255

DHCP REQUEST

Source IP : 0.0.0.0

Destination IP : 255.255.255.255

DHCP ACK

Source IP : 192.168.1.254

Destination IP : 255.255.255.255

Câu hỏi 5 : Gói tin nào chứa địa chỉ IP mà Server muốn cấp cho máy client :

Ta có thể thấy gói DHCP OFFER mà máy DHCP server gửi cho client chứa các thông tin về địa chỉ IP của client cũng như các phần phụ thêm như Subnet mask, DNS IP ...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xef9b2257
2	0.001855	192.168.1.254	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xef9b2257
3	0.002113	0.0.0.0	255.255.255.255	DHCP	368	DHCP Request - Transaction ID 0xef9b2257
4	0.003288	192.168.1.254	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xef9b2257
15	4.118689	192.168.1.10	192.168.1.254	DHCP	356	DHCP Request - Transaction ID 0xc2863620
16	4.119238	192.168.1.254	192.168.1.10	DHCP	342	DHCP ACK - Transaction ID 0xc2863620
30	10.479522	192.168.1.10	192.168.1.254	DHCP	342	DHCP Release - Transaction ID 0x5be56aa1
31	15.211450	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x11afb4ec
32	15.211901	192.168.1.254	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x11afb4ec
33	15.212107	0.0.0.0	255.255.255.255	DHCP	368	DHCP Request - Transaction ID 0x11afb4ec
34	15.212532	192.168.1.254	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x11afb4ec

```

Hardware address length: 6
Hops: 0
Transaction ID: 0xef9b2257
Seconds elapsed: 0
+ Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (Client) IP address: 192.168.1.10 (192.168.1.10)
Next server IP address: 192.168.1.254 (192.168.1.254)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: vmware_5b:ef:6a (00:0c:29:5b:ef:6a)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
+ Option: (t=53,l=1) DHCP Message Type = DHCP Offer
+ Option: (t=1,l=4) Subnet Mask = 255.255.255.0
+ Option: (t=58,l=4) Renewal Time Value = 4 days
+ Option: (t=59,l=4) Rebinding Time Value = 7 days
+ Option: (t=51,l=4) IP Address Lease Time = 8 days
+ Option: (t=54,l=4) DHCP Server Identifier = 192.168.1.254
+ Option: (t=6,l=4) Domain Name Server = 8.8.8.8
End option
Padding

```

I.

Gói tin trên chứa các thông tin cơ bản sau :

- Địa chỉ IP Client 192.168.1.10
- Subnet Mask 255.255.255.0
- DHCP Server 192.168.1.254
- DNS Server 8.8.8.8
- Lease Time 8 days
- ...

Câu hỏi 6 : Địa chỉ IP mà Client muốn DHCP cấp trong gói DHCP REQUEST :

1	0.000000	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover	- Transaction ID 0xef9b2257
2	0.001855	192.168.1.254	255.255.255.255	DHCP	342	DHCP Offer	- Transaction ID 0xef9b2257
3	0.002113	0.0.0.0	255.255.255.255	DHCP	368	DHCP Request	- Transaction ID 0xef9b2257
4	0.003288	192.168.1.254	255.255.255.255	DHCP	342	DHCP ACK	- Transaction ID 0xef9b2257
15	4.118689	192.168.1.10	192.168.1.254	DHCP	356	DHCP Request	- Transaction ID 0xc2863620
16	4.119238	192.168.1.254	192.168.1.10	DHCP	342	DHCP ACK	- Transaction ID 0xc2863620
30	10.479522	192.168.1.10	192.168.1.254	DHCP	342	DHCP Release	- Transaction ID 0x5be56aa1
31	15.211450	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover	- Transaction ID 0x11afb4ec
32	15.211901	192.168.1.254	255.255.255.255	DHCP	342	DHCP Offer	- Transaction ID 0x11afb4ec
33	15.212107	0.0.0.0	255.255.255.255	DHCP	368	DHCP Request	- Transaction ID 0x11afb4ec
34	15.212532	192.168.1.254	255.255.255.255	DHCP	342	DHCP ACK	- Transaction ID 0x11afb4ec

```

Bootstrap Protocol
  Message type: Boot Request (1)
  Hardware type: Ethernet
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xef9b2257
  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: vmware_5b:ef:6a (00:0c:29:5b:ef:6a)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  Option: (t=53,l=1) DHCP Message Type = DHCP Request
  Option: (t=61,l=7) Client identifier
  Option: (t=50,l=4) Requested IP Address = 192.168.1.10
  Option: (t=54,l=4) DHCP Server Identifier = 192.168.1.254
  Option: (t=43,l=15) Vendor Specific Information

```

Sau khi nhận được thông tin về địa chỉ IP DHCP Server mong muốn cấp tại gói DHCP OFFER. Client sẽ xác nhận nó muốn nhận địa chỉ IP nào ở gói tin DHCP REQUEST.

ở đây địa chỉ đó là: **192.168.1.10**.

Câu hỏi 7 : Gói tin nào chứa địa chỉ IP mà Server sẽ cấp cho Client :

Đây là gói cuối cùng, xác định các thông tin đã thỏa thuận giữa Server và Client trong suốt quá trình trao đổi cũng như là gói tin cuối cùng trong quá trình giao tiếp DHCP có tên gọi DHCP ACK.

VMware Accelerated AMD PCNet Adapter (Microsoft's Packet Scheduler) [Wireshark 1.6.1 (SVN Rev 38096 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: bootp Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xef9b2257
2	0.001855	192.168.1.254	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xef9b2257
3	0.002113	0.0.0.0	255.255.255.255	DHCP	368	DHCP Request - Transaction ID 0xef9b2257
4	0.003288	192.168.1.254	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xef9b2257
15	4.118689	192.168.1.10	192.168.1.254	DHCP	356	DHCP Request - Transaction ID 0xc2863620
16	4.119238	192.168.1.254	192.168.1.10	DHCP	342	DHCP ACK - Transaction ID 0xc2863620
30	10.479522	192.168.1.10	192.168.1.254	DHCP	342	DHCP Release - Transaction ID 0x5be56aa1
31	15.211450	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x11afb4ec
32	15.211901	192.168.1.254	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x11afb4ec
33	15.212107	0.0.0.0	255.255.255.255	DHCP	368	DHCP Request - Transaction ID 0x11afb4ec
34	15.212532	192.168.1.254	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x11afb4ec

Message type: Boot Reply (2)
 Hardware type: Ethernet
 Hardware address length: 6
 Hops: 0
 Transaction ID: 0xef9b2257
 Seconds elapsed: 0
 Bootp flags: 0x0000 (Unicast)
 Client IP address: 0.0.0.0 (0.0.0.0)
 Your (client) IP address: 192.168.1.10 (192.168.1.10)
 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: vmware_5b:ef:6a (00:0c:29:5b:ef:6a)
 Client hardware address padding: 00000000000000000000
 Server host name not given
 Boot file name not given
 Magic cookie: DHCP
 Option: (t=53,l=1) DHCP Message Type = DHCP ACK
 Option: (t=58,l=4) Renewal Time Value = 4 days
 Option: (t=59,l=4) Rebinding Time Value = 7 days
 Option: (t=51,l=4) IP Address Lease Time = 8 days
 Option: (t=54,l=4) DHCP Server Identifier = 192.168.1.254
 Option: (t=1,l=4) Subnet Mask = 255.255.255.0
 Option: (t=81,l=3) Client Fully Qualified Domain Name

Tài liệu tham khảo

<http://www.wikipedia.org/>

<http://technet.microsoft.com/>

<http://www.nhatnghe.com/>