

# Simulasi dan Monitoring DHCP

**Imam Prasetyo**

*imp.masiv@gmail.com*

*http://superman-kartini.blogspot.com*

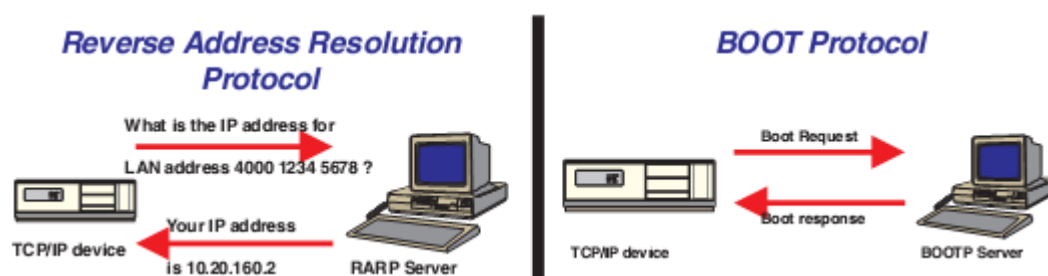
## **Lisensi Dokumen:**

Copyright © 2003-20013 IlmuKomputer.Com

Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

## **Pendahuluan**

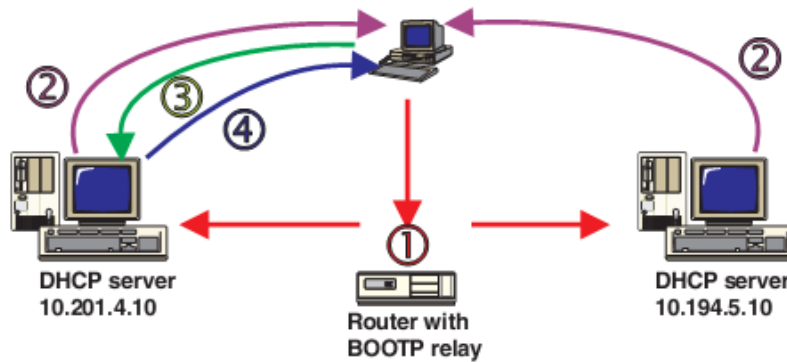
DHCP (Dynamic Host Configuration Protocol) adalah protokol layer aplikasi yang digunakan untuk mengalokasikan IP address secara automatic dan dinamicly pada host di suatu jaringan komputer. Protokol ini berjalan diatas protokol RARP (Reverse Address Resolution Protocol) dan BOOTP (Bootstrap Protocol). Dimana ARP itu sendiri adalah protokol yang digunakan untuk mengetahui MAC address suatu host yang notabennya IP (logical address)-nya diketahui. Dengan begitu dapat diketahui bahwa RARP bekerja sebaliknya. Berikut ini merupakan gambar analogi dari RARP dan BOOTP.



Pada dasarnya ada tiga metode dalam DHCP, yaitu :

- Manual → seperti BOOTP
- Automatic → alamat IP dialokasikan dari pool dan diasosiasikan dengan MAC address hingga ada intervensi atau pemutusan jaringan manual
- Dynamic → alamat IP dialokasikan dari pool untuk waktu yang spesifik (ada leased period)

Secara umum operasi DHCP dapat dilihat pada gambar dibawah.



1. Host submit pesan DHCP request IP address discover.
2. Mungkin lebih dari 1 server akan merespon
3. Host memilih satu alamat IP yang ditawarkan server
4. Server memberikan alamat IP tersebut

Untuk memahami DHCP lebih dalam ada baiknya mengetahui isi dari header atau message format DHCP, analoginya adalah gambar dibawah.

0	7	15	23	31
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)				
options (variable)				

Berikut ini adalah penjelasannya :

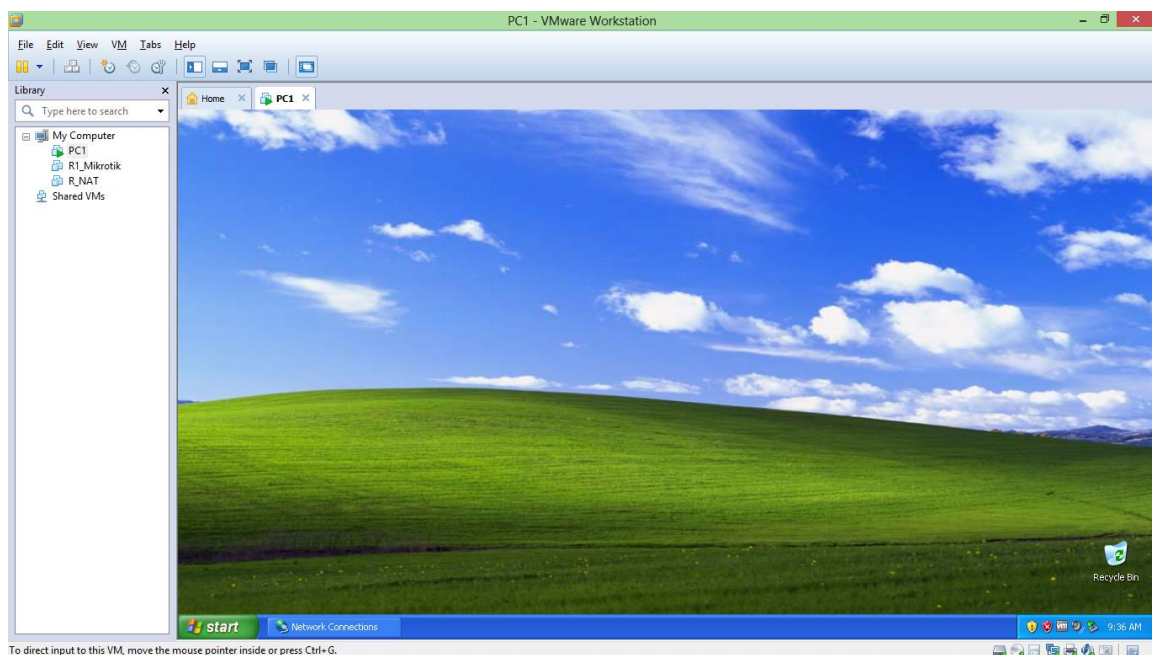
- Op : Tipe pesan, 1 untuk REQUEST dan 2 untuk REPLY
- Htype, hlen : Tipe dan panjang alamat hardware DHCP client.
- Hops : nomor dari relay agent
- Xid : ID transaksi, nomor acak 32 bit yang dipilih klien untuk mengidentifikasi alokasi IP address.
- Secs : waktu yang digunakan klien sejak dia memulai.

- Flags : mengindikasikan DHCP server dibalas dari broadcast atau unicast.
- Ciaddr : IP address klien.
- Yiaddr : “your” (klien) IP address, diberikan oleh server.
- Siaddr : Server IP address, yang mengkonfigurasi alokasi IP.
- Giaddr : IP dari relay agent pertama
- Chaddr : alamat hardware klien
- Sname : server hostname
- File : nama dari bootfile dan informasi routing.
- Options : parameter opsional.

## Simulasi DHCP

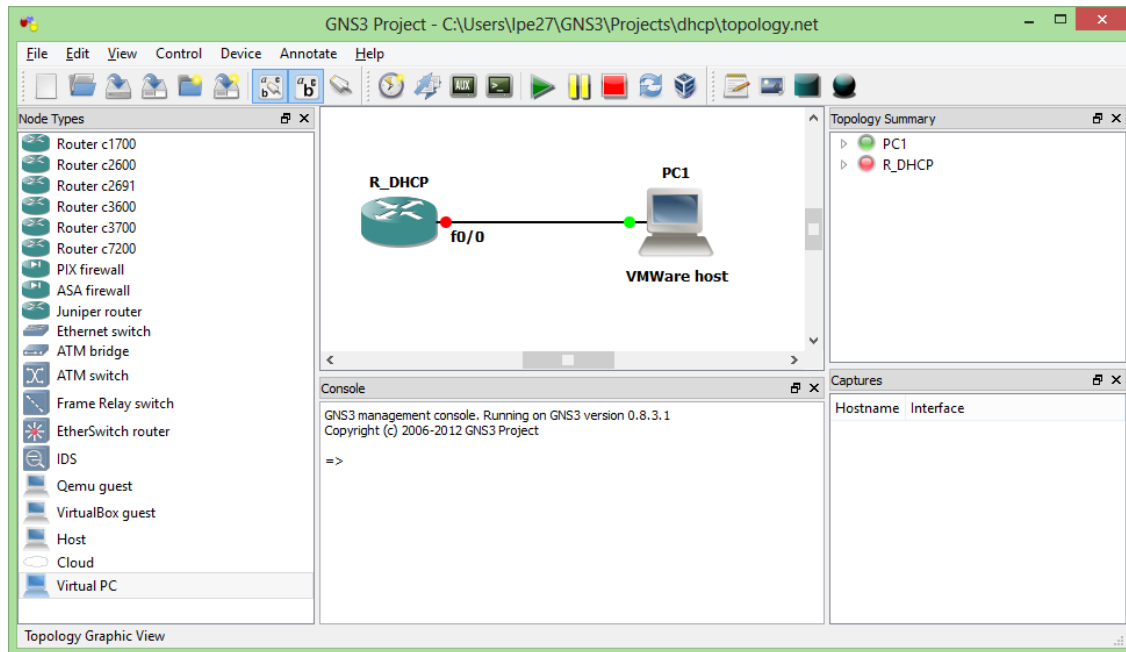
Simulasi yang dilakukan adalah menggunakan aplikasi GNS3. Mengkonfigurasi router sebagai DHCP server kemudian sebuah klien (berupa host di VMWare) akan meminta koneksi DHCP terhadapnya. Berikut ini adalah langkah-langkah simulasinya.

1. Buka dan hidupkan virtual PC pada VMWare yang akan dijadikan sebagai host.

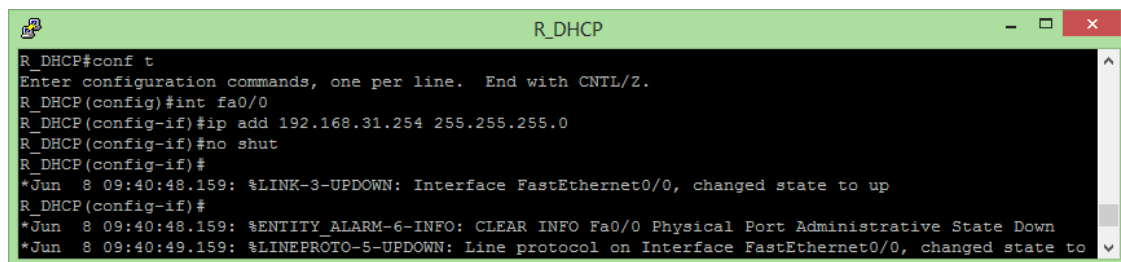


NB : Network adapter tipenya “host only” karena jaringannya hanya sebatas virtual dalam satu PC saja.

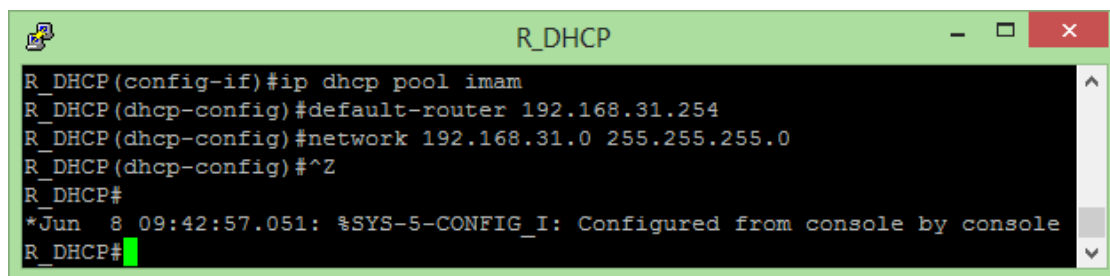
2. Buatlah topologi jaringan komputer pada GNS3 seperti gambar berikut.



3. Konfigurasi interface Router DHCP agar “up” seperti gambar berikut.



4. Konfigurasi pool R\_DHCP agar bisa menjadi server DHCP pada jaringan yang terhubung fa0/0.



Command :

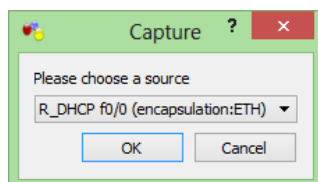
- #interface <nama interface yang digunakan>
- #ip dhcp pool <nama>
- #default-router <IP gateway>
- #network <IP network> <subnet mask>

5. Berikutnya adalah memberi alamat IP Host VMWare. Karena menggunakan DHCP kita tidak perlu konfigurasi manual. Pada pembahasan berikutnya akan dijelaskan bagaimana mengkonfigurasi secara otomatis.

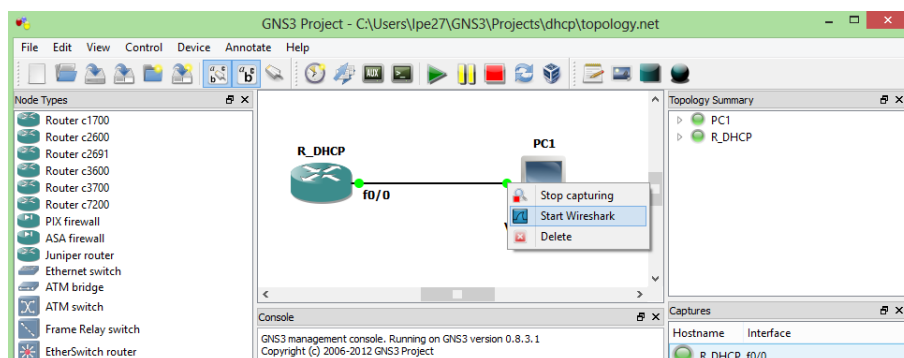
## Monitoring DHCP

Dari topologi yang telah dibuat tadi, Host VMWare akan melakukan DHCP untuk mendapatkan parameter IP secara dinamic dan auomatically seperti yang telah dijelaskan di pendahuluan. Berikut ini adalah langkah-langkahnya dan monitoringnya.

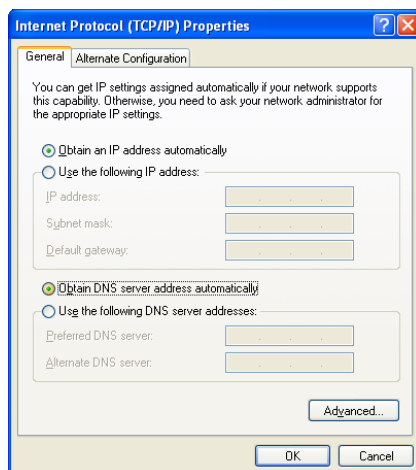
1. Pada topologi tadi klik kanan pada koneksi PC1 dan Router kemudian pilih “start capture”. Saat muncul notifikasi klik “ok”.



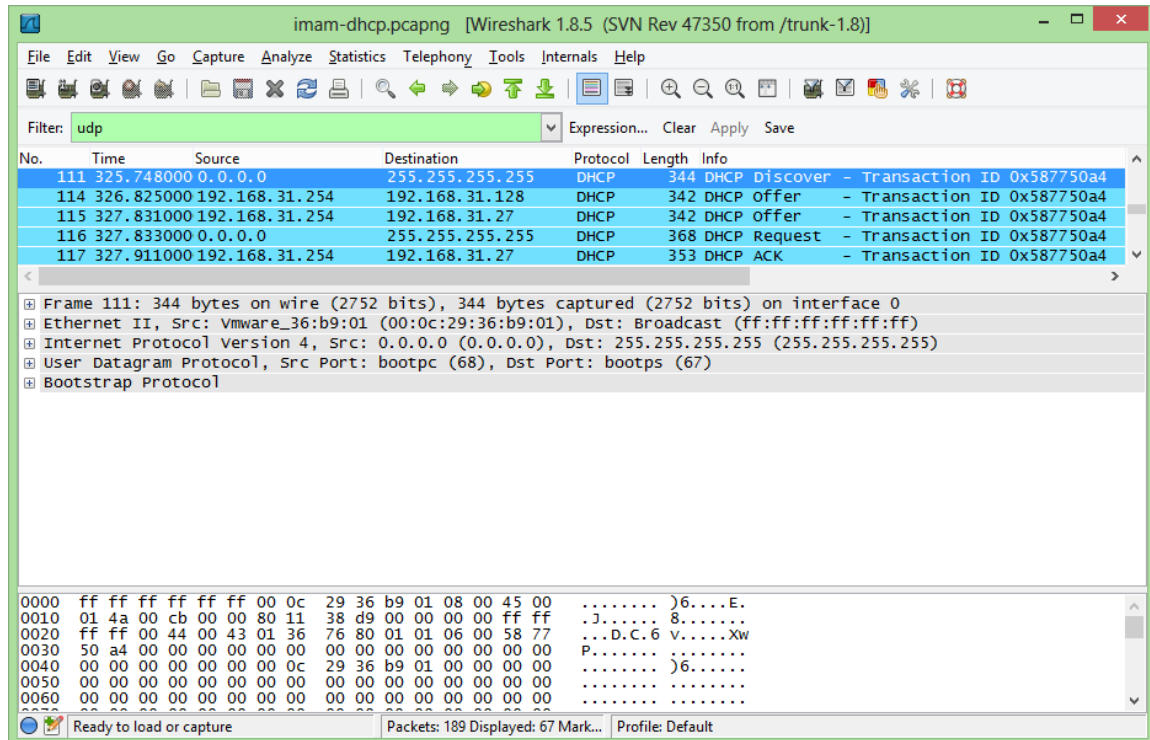
2. Pada sambungan antara device, klik kanan dan pilih “start wireshark”.



3. Pada virtual PC1 VMWare, konfigurasi interfacenya agar memperoleh IP otomatis dari server DHCP.

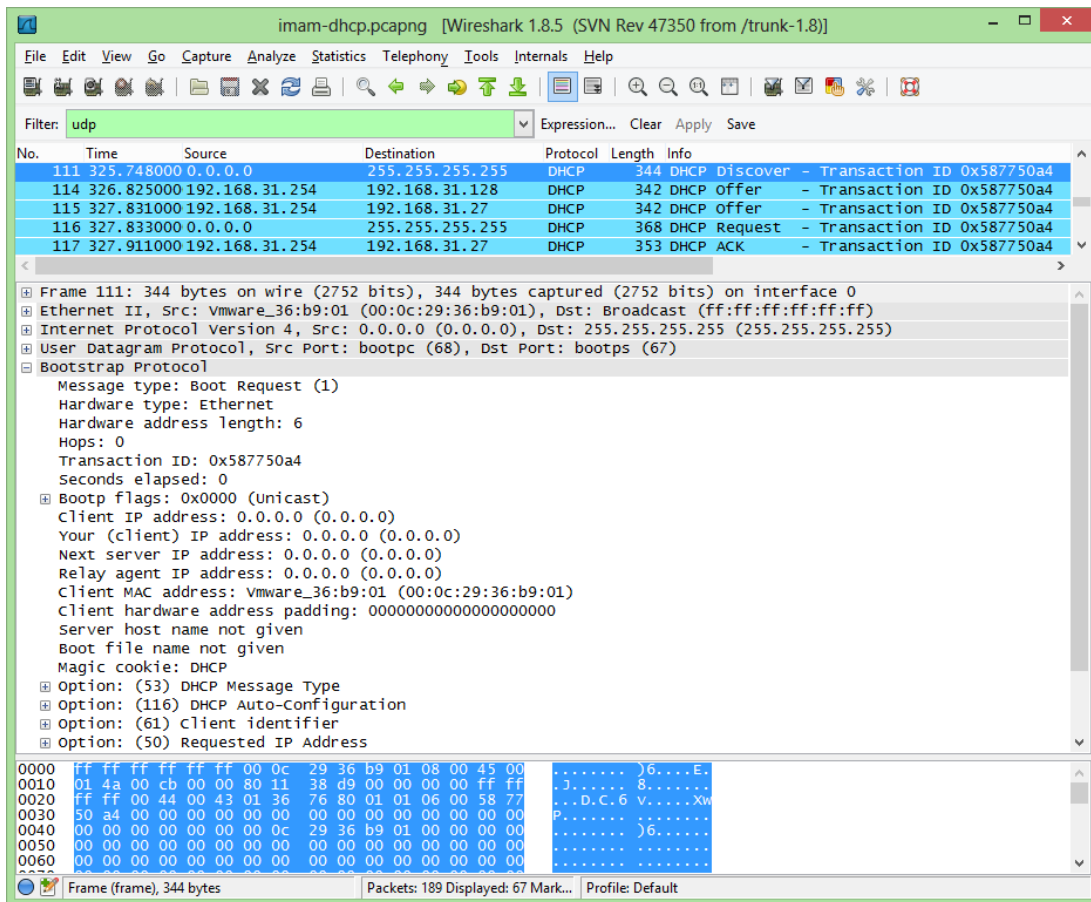


4. Bukalah wireshark yang digunakan untuk mengcapture tadi kemudian buatlah filter “UDP” (protokol transport yang digunakan DHCP).



Nah dapat dilihat ada 4 buah tipe pesan yang digunakan pada DHCP yaitu DHCP discover, DHCP Offer, DHCP Request, dan DHCP ACK. Pada pembahasan berikutnya akan dibahas lebih detil mengenai keempat proses tersebut.

 DHCP discover



The image shows a Wireshark capture of a DHCP discover packet. The packet list pane shows five packets related to a DHCP transaction with ID 0x587750a4:

No.	Time	Source	Destination	Protocol	Length	Info
111	325.748000	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x587750a4
114	326.825000	192.168.31.254	192.168.31.128	DHCP	342	DHCP Offer - Transaction ID 0x587750a4
115	327.831000	192.168.31.254	192.168.31.27	DHCP	342	DHCP Offer - Transaction ID 0x587750a4
116	327.833000	0.0.0.0	255.255.255.255	DHCP	368	DHCP Request - Transaction ID 0x587750a4
117	327.911000	192.168.31.254	192.168.31.27	DHCP	353	DHCP ACK - Transaction ID 0x587750a4

The packet details pane for frame 111 shows the following information:

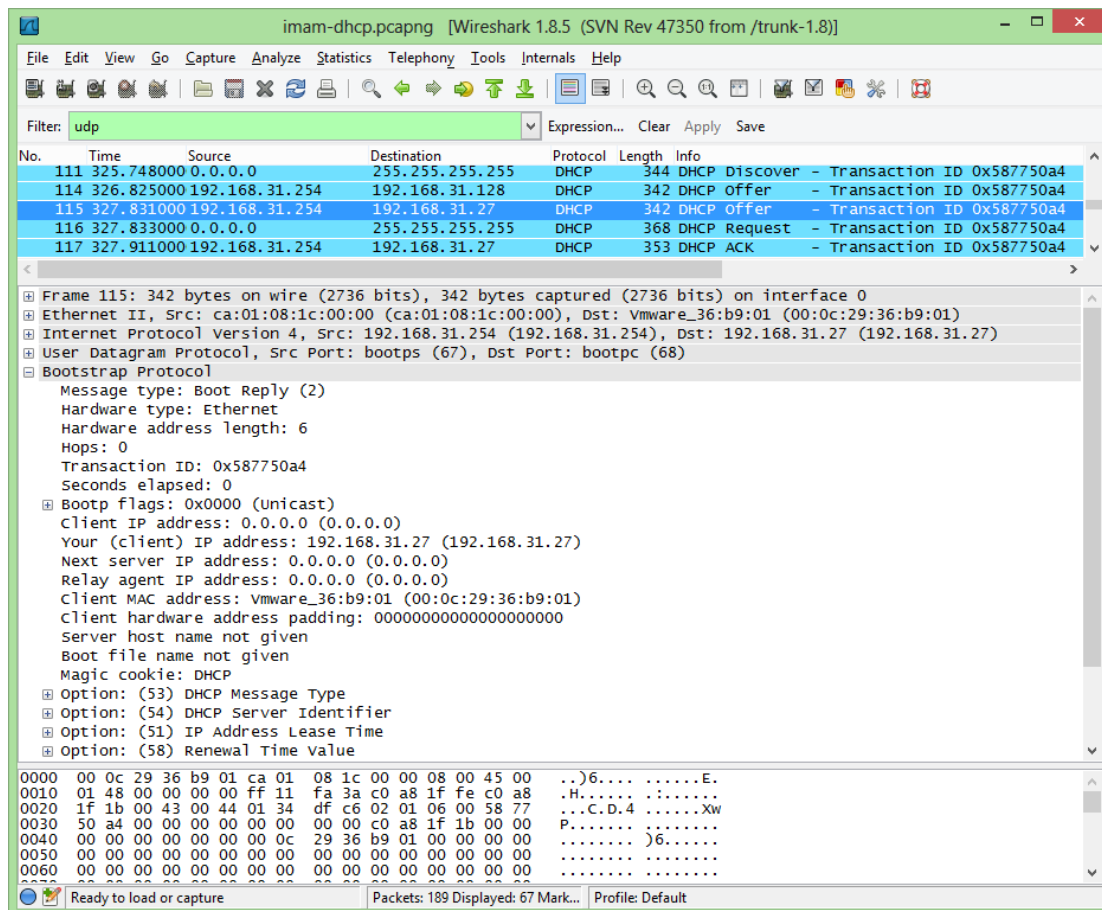
- Frame 111: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface 0
- Ethernet II, Src: Vmware\_36:b9:01 (00:0c:29:36:b9:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
- User Datagram Protocol, 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: 0x587750a4
  - 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\_36:b9:01 (00:0c:29:36:b9:01)
  - Client hardware address padding: 00000000000000000000
  - Server host name not given
  - Boot file name not given
  - Magic cookie: DHCP
  - Option: (53) DHCP Message Type
  - Option: (116) DHCP Auto-configuration
  - Option: (61) Client identifier
  - Option: (50) Requested IP Address

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, IP header, and UDP header.

Pesan DHCP discover ini dikirimkan dari klien (PC1 dengan MAC : Vmware\_36:b9:01) ke alamat broadcast (255.255.255.255) yang tujuannya meminta IP address secara otomatis. Dapat dilihat messages tipe-nya adalah 1 (boot request). Kemudian flagnya adalah unicast (berasal dari 1 sumber yaitu PC1). Pada pesan broadcast ini semua alamat (baik logic maupun fisik) dari server dan klien belum diketahui kecuali alamat fisik klien (PC1)

 DHCP Offer





Pesan DHCP offer ini adalah pesan yang dikirimkan oleh server DHCP (R\_DHCP IP : 192.168.31.254 MAC : ca:01:08:1c:00:00) yang “menawarkan” parameter IP address secara otomatis dan dinamicly tadi kepada klien (PC1). Dapat dilihat pesan ini bertipe 2 (boot reply), flagnya unicast, dan IP yang ditawarkan ada dua yaitu 192.168.31.128 dan 192.168.31.27.

#### DHCP request



The screenshot displays a DHCP transaction in Wireshark. The packet list shows:

No.	Time	Source	Destination	Protocol	Length	Info
111	325.748000	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x587750a4
114	326.825000	192.168.31.254	192.168.31.128	DHCP	342	DHCP offer - Transaction ID 0x587750a4
115	327.831000	192.168.31.254	192.168.31.27	DHCP	342	DHCP offer - Transaction ID 0x587750a4
116	327.833000	0.0.0.0	255.255.255.255	DHCP	368	DHCP Request - Transaction ID 0x587750a4
117	327.911000	192.168.31.254	192.168.31.27	DHCP	353	DHCP ACK - Transaction ID 0x587750a4

The details pane for frame 116 shows:

- Frame 116: 368 bytes on wire (2944 bits), 368 bytes captured (2944 bits) on interface 0
- Ethernet II, Src: Vmware\_36:b9:01 (00:0c:29:36:b9:01), 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)
- 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: 0x587750a4
  - 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\_36:b9:01 (00:0c:29:36:b9:01)
  - Client hardware address padding: 00000000000000000000
  - Server host name not given
  - Boot file name not given
  - Magic cookie: DHCP
  - Option: (53) DHCP Message Type
  - Option: (61) Client identifier
  - Option: (50) Requested IP Address
  - Option: (54) DHCP Server Identifier

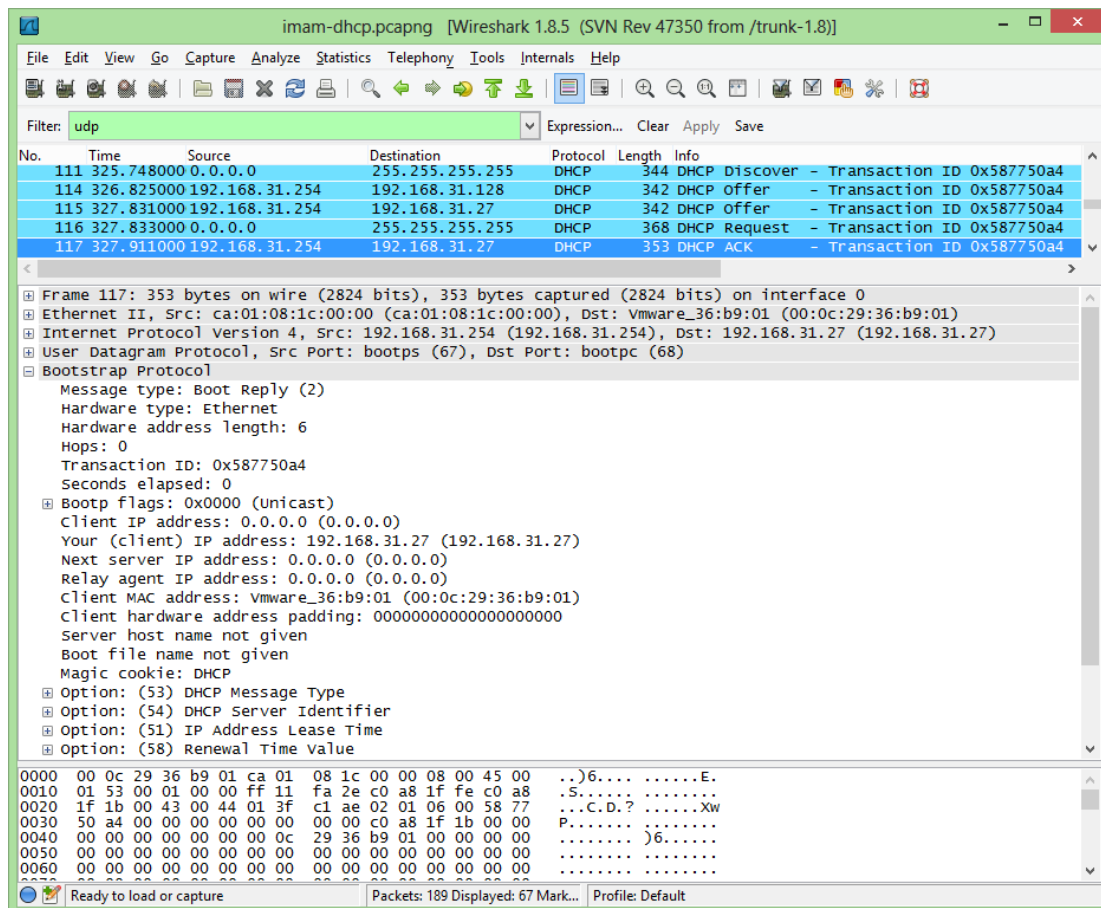
The packet bytes pane shows the raw data in hexadecimal and ASCII:

```

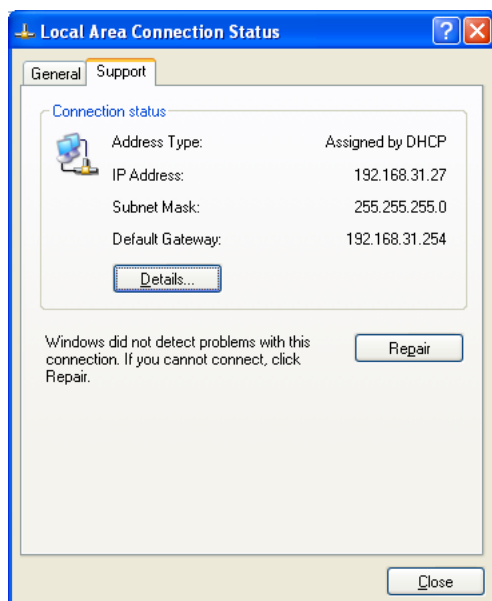
0000 ff ff ff ff ff ff 00 0c 29 36 b9 01 08 00 45 00 ..... )6....E.
0010 01 62 00 cc 00 00 80 11 38 c0 00 00 00 00 ff ff .b..... 8.....
0020 ff ff 00 44 00 43 01 4e ce 31 01 01 06 00 58 77 ...D.C.N .1....Xw
0030 50 a4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 P.....
0040 00 00 00 00 00 00 00 00 0c 29 36 b9 01 00 00 00 ..... )6.....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
    
```

Pesan DHCP request ini adalah dari klien (PC1) meminta parameter IP yang telah ditawarkan dari server tadi (DHCP offer). Message tipenya adalah request, bootp flag-nya adalah unicast.

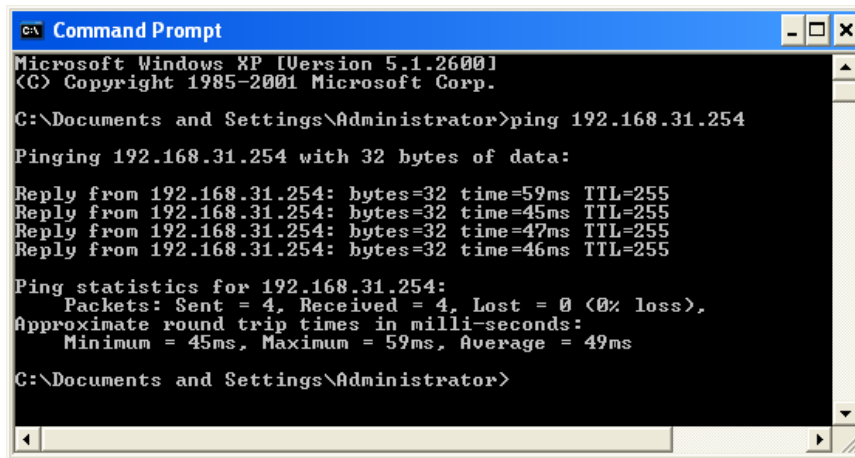
#### DHCP ACK



DHCP ACK adalah pesan yang dikirimkan oleh server (R\_DHCP) ke klien (PC1) berisi parameter IP yang akan digunakan pada klien. Dapat dilihat bahwa IP yang diberikan pada klien (PC1) yang beralamat fisik Vmware\_36:b9:01 adalah 192.168.31.27. Dengan ini kita tidak perlu mengkonfigurasi IP PC1 secara manual. Dapat dilihat di detail koneksi pada PC1 VMWare bahwa DHCP telah berjalan dengan baik.



Berikut ini adalah screenshot ping dari PC1 ke R\_DHCP



```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.31.254

Pinging 192.168.31.254 with 32 bytes of data:

Reply from 192.168.31.254: bytes=32 time=59ms TTL=255
Reply from 192.168.31.254: bytes=32 time=45ms TTL=255
Reply from 192.168.31.254: bytes=32 time=47ms TTL=255
Reply from 192.168.31.254: bytes=32 time=46ms TTL=255

Ping statistics for 192.168.31.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 45ms, Maximum = 59ms, Average = 49ms

C:\Documents and Settings\Administrator>
```

Topologi dan capture wireshark yang saya buat diatas dapat anda download di →

<http://www.mediafire.com/?04p96w4adw43vea>

## Biografi Penulis



**Imam Prasetyo.** Kuliah D4 Teknik Telekomunikasi di Politeknik Negeri Semarang. Lulusan SMA Negeri 1 Pati tahun 2010 dan SMP Negeri 1 Pati tahun 2007. Dari kecil sangat tertarik pada ilmu pengetahuan alam dan teknologi. Untuk informasi maupun tulisan menarik lain dapat diakses di situs blog <http://www.superman-kartini.blogspot.com>