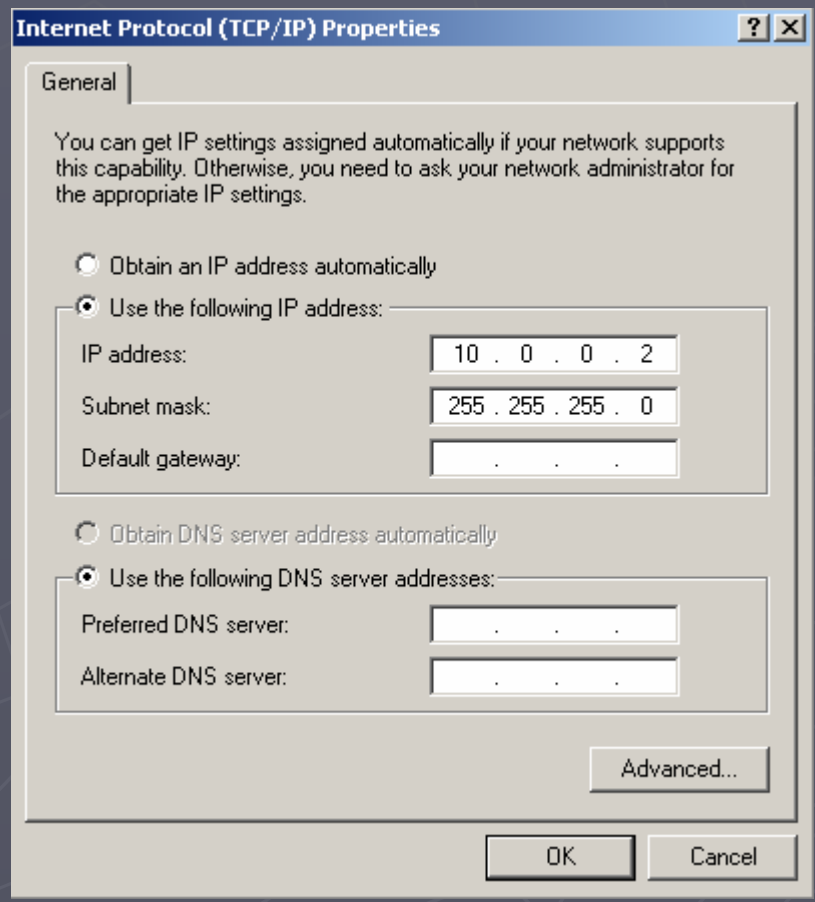
DHCP Server
Konsep dan Penerapan

Oleh
Tim Network Administrator PENS ITS

Politeknik Elektronikan Negeri Surabaya
Institut Tekonolgi Sepuluh Nopember
Surabaya

Pendahuluan

- Alamat IP (IP Address; sering disingkat IP) adalah angka 32-bit yang menunjukkan alamat dari sebuah komputer pada jaringan berbasis TCP/IP.
- Pengiriman data dalam jaringan TCP/IP berdasarkan IP address komputer pengirim dan komputer penerima.



Pendahuluan (Lanj..)

- Pengalamatan IP address
  - IP Statis
    Konfigurasi IP secara Manual
  - IP dinamis
    Konfigurasi IP Oleh Computer Server melalui Jaringan Computer

- DHCP (Dynamic Host Configuration Protocol)
  - Merupakan protokol yang dipakai untuk pengalokasian alamat IP (IP address) dalam satu jaringan.
  - Jika Non DHCP, pemberian alamat IP manual satu persatu ke sel. Komputer
  - Jika menggunakan DHCP, seluruh komputer yang tersambung di jaringan akan mendapatkan alamat IP secara otomatis dari server DHCP.
  - Selain alamat IP, banyak parameter jaringan yang dapat diberikan oleh DHCP, seperti default gateway dan DNS server.

Pendahuluan (Lanj..)

- DHCP merupakan Standar dari IETF (Internet Engineering Task Force)
- Dikembangkan tahun 1993, sbg perbaikan dan BOOTP (Bootstrap Protocol)
  - RFC 2131: Dynamic Host Configuration Protocol
    - Lihat dokumen
  - RFC 2132: DHCP Options and BOOTP Vendor Extensions
    - Lihat dokumen

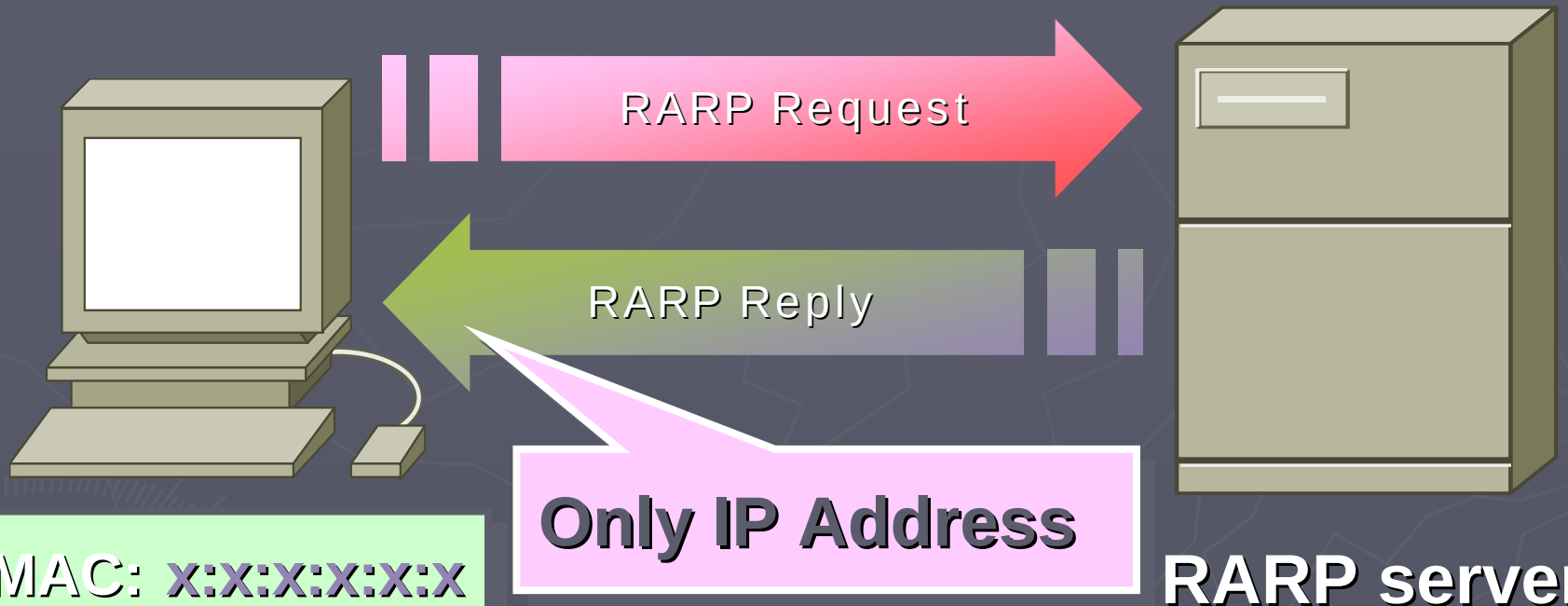
Kenapa Butuh DHCP Server ?

- Jaringan semakin besar dan semakin komplek sehingga butuh konfigurasi secara dinamis
  - Bayangkan jika kita punya 100 komputer atau lebih terhubung di jaringan dan harus konfigurasi satu persatu
- Pengendalian parameter komputer client
  - IP dan default router/gateway
  - Name Server
  - File Server
  - dll (*Default IP TTL, Broadcast Address, Static Route, Ethernet Encapsulation, X Window Manager, X Window Font, DHCP Msg Type, DHCP Renewal Time, DHCP Rebinding, Time SMTP-Server, SMTP-Server, Client FQDN, Printer Name, ...)*
- Pengiriman informasi tanpa admin, tidak perlu konfigurasi tiap komputer, Tidak ada manual konfigurasi di client
- Host-host yang terkonfigurasi secara statis bisa berdampingan dengan yang dinamis

Sejarah DHCP Server

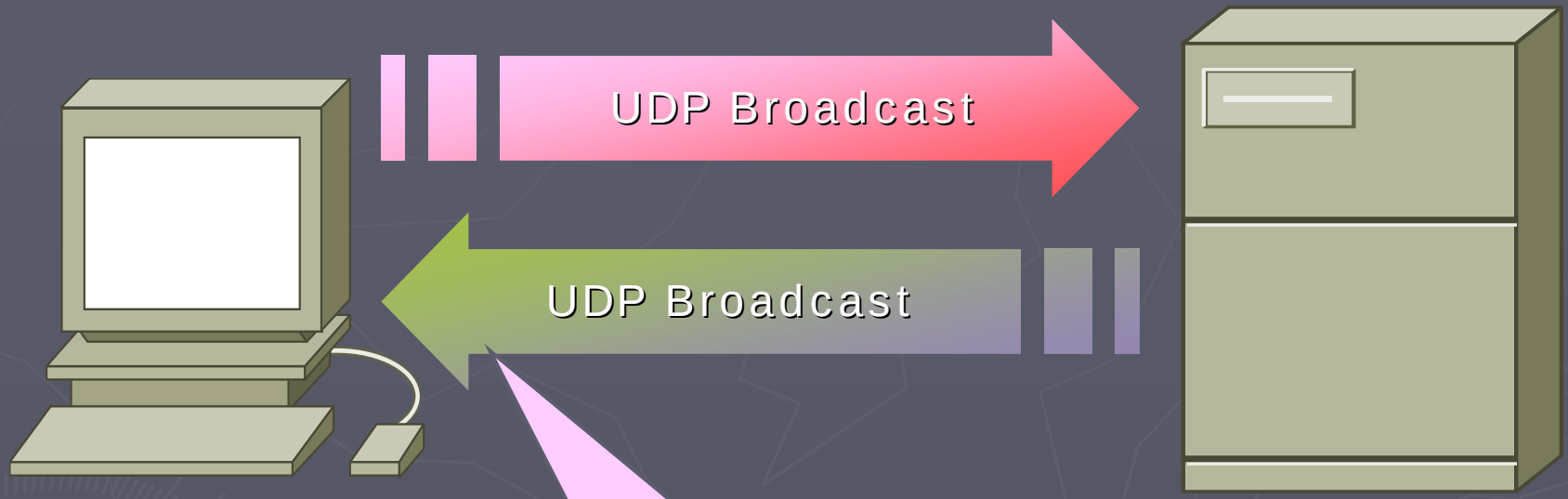
- Tiga Protocol yang pernah dipakai untuk penanganan IP secara dinamis
  - RARP (s/d 1985, tidak lama digunakan)
    - Reverse Address Resolution Protocol
  - BOOTP (1985-1993)
    - Bootsrap Protocol
  - DHCP (sejak 1993 sampai sekarang)
    - Dynamic Host Configuration Protocol
- Hanya DHCP yang sekarang dipakai secara luas

System Kerja RARP



MAC HEADER	IP HEADER	RARP REQUEST MESSAGE
Destination 08-00-02-89-90-8 Source 02-60-8C-01-02-03	Destination 11111111 Source ????????	What is my IP address?

Sistem Kerja BOOTP



MAC: x:x:x:x:x:x
IP: ?

IP Address
Gateway
IP server
Vendor-specific

BOOTP server

MAC1 – IP1
MAC2 – IP2
MAC3 – IP3

RFC 2131

- RFC (Requets For comments) adalah aturan-aturan yang telah ditetapkan secara umum untuk mengatur proses apa saja seputar internet.
- RFC 2131 adalah berisi aturan-aturan atau protocol yang digunakan pada proses DHCP
- Pada RFC 2131 ini dijelaskan bagaimana dan apa yang dilakukan oleh DHCP server dan DHCP client ketika menggunakan protocol ini

Format Paket DHCP

- Ide dasar memberikan IP ke client, server harus ingat IP tersebut dan parameternya.
- Yang dikirim bukan Cuma IP tapi juga parameter - parameter
- Jika client booting sedapatkan mungkin diberi IP yang sama.

System DHCP

- Binding/lease (kumpulan 1 IP dan 1 client)
- Client menyewa dalam waktu tertentu
- Jika waktu habis harus menyewa kembali.
- Dua timer :
  - Renewing (T1)
  - Rebinding (T2)
- T1 ditentukan terlebih dahulu
- T1 : ½ T2

DHCP Message

- DHCPDISCOVER
  - Ini merupakan tipe pertama dari DHCP, yang menentukan klien broadcast untuk menemukan server DHCP lokal. Opsi Message Type dikodekan ‘1
- DHCPOFFER
  - Server DHCP yang menerima satu klien DHCPDISCOVER dan yang dapat melayani permintaan operasi, mengirim DHCPOFFER pada klien dengan sekumpulan parameter. Opsi Messsage Type dikodekan ‘2’
- DHCPREQUEST
  - Klien menerima satu atau lebih DHCPOFFER dan memutuskan tawaran yang diterima. Klien kemudian mengirim tawaran DHCPREQUEST ke “pemenang”. Semua server yang lain mengetahui pesan broadcast ini dan dapat memutuskan bahwa mereka “kalah”. Opsi Message Type dikodekan ‘3’.
- DHCPACK
  - Akhirnya server mengirim DHCPACK ke klien dengan sekumpulan parameter konfigurasi, mengkonfirmasi pada klien bahwa DHCPREQUEST diterima, dan memberikan kumpulan informasi yang diperlukan. Bagian ACK dari nama pesan ini kependekan dari “*acknowledge*”. Opsi Message Type dikodekan ‘5’

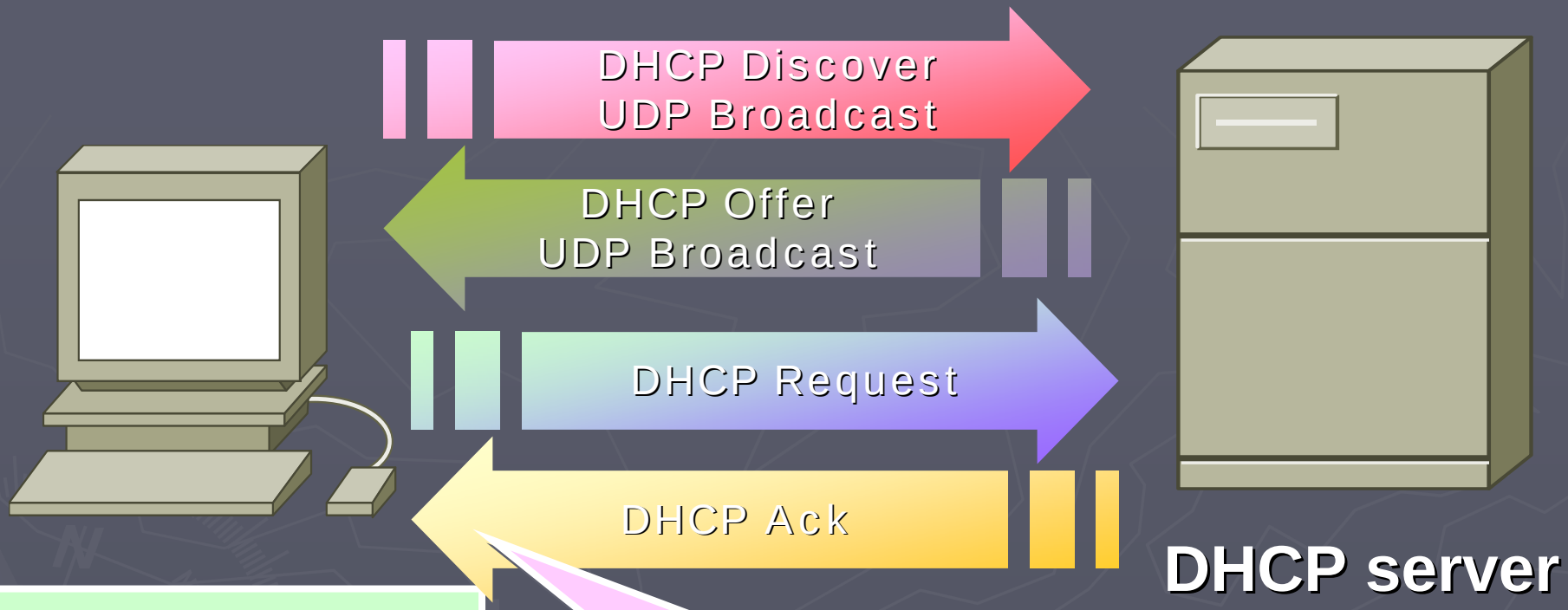
DHCP Message

- DHCPNACK
  - Jika klien meminta (dengan pesan DHCPREQUEST) alamat yang salah, kadaluwarsa, atau yang lainnya yang tidak dapat diterima, maka server mengirim DHCPNAK ke klien untuk memberitahu bahwa ia tidak dapat memperoleh alamat tersebut. 'NAK" dalam hal ini kependekan dari "*negative acknowledge*". Opsi Message Type dikodekan '5'
- DHCPDECLINE
  - Jika klien menerima alamat yang diminta, dan secara berturutan menemukan bahwa alamat itu telah digunakan ditempat lain dalam jaringan, ia harus mengirim DHCPDECLINE ke server. Klien mungkin mencoba mengirim suara ke alamat. Jika ada jawaban berarti ada orang yang menggunakan alamat server. Opsi Message Type dikodekan '4'
- DHCPRELEASE
  - Jika klien tidak lagi perlu menggunakan alamat yang ditunjuk secara dinamis, ia harus mengirim pesan DHCPRELEASE ke server supaya server mengetahui bahwa alamat tidak lagi digunakan. Tidak semua klien DHCP melakukan hal ini karena merupakan pilihan teknis. Opsi Message Type dikodekan '7'
- DHCPINFORM
  - Jika klien telah mempunyai alamat IP, tetapi masih memerlukan beberapa informasi konfigurasi, maka pesan DHCPINFORM akan melayani tugas ini. Opsi Message Type dokodekan '8'.

Aturan dan Proses RFC 2131

- Ketika DHCP client masuk/bergabung kedalam suatu jaringan, client tesebut akan melakukan broadcast dengan mengirimkan pesan DHCPDISCOVER ke suatu network.
- Seluruh DHCP server akan merespon DHCPDISCOVER yang dikirimkan DHCP client tersebut dengan DHCPOFFER.
- Ketika client mendapatkan DHCPOFFER, client memiliki dua pilihan keputusan yaitu, mengirimkan DHCPREQUEST untuk menerima konfigurasi dari DHCP server
- Ketika DHCP server menerima DHCPREQUEST, DHCP server dapat mengirimkan DHCPACK dengan membawa parameter-parameter konfigurasi untuk client dan memasukkan informasi itu kedalam *dhcp.lease* database jika DHCP Server menyetujui DHCPREQUEST dari Client atau DHCP Server mengirimkan DHCPNACK ataui dengan tidak merespon pesan DHCPREQUEST jika DHCP Server tidak menyetujuinya
- Jika DHCP client telah selesai atau meninggalkan jaringan tersebut maka DHCP client mengirimkan pesan DHCPRELEASE sebagai tanda bahwa client telah keluar atau tidak menggunakan network address tersebut. Namun tidak semua sistem operasi yang melakukan ini

Sistem Kerja DHCP

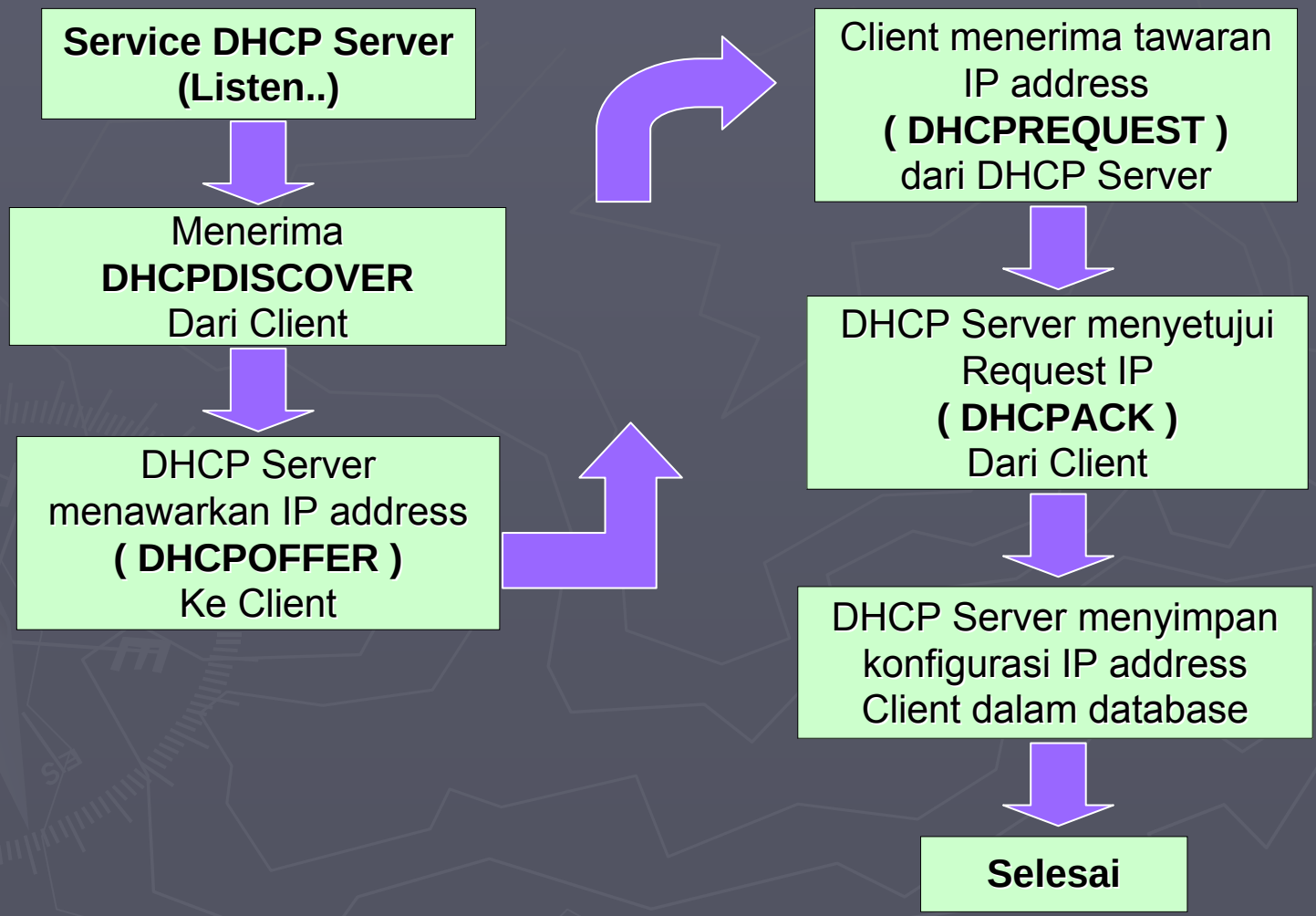


MAC: x:x:x:x:x:x
IP: ?

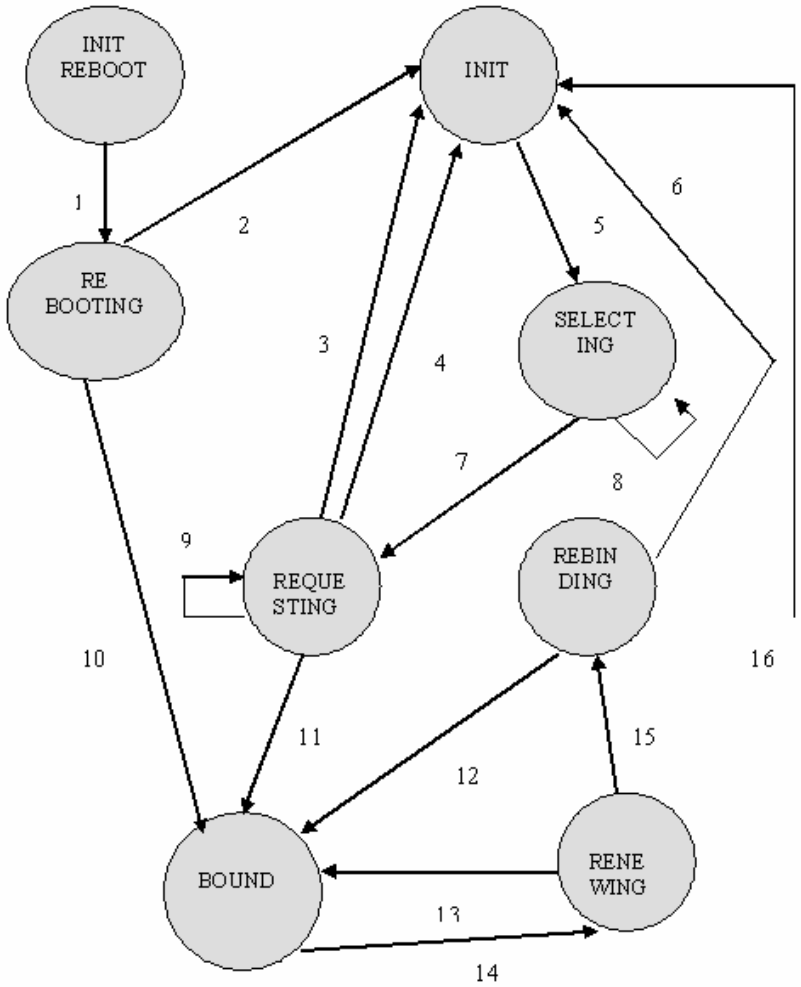
IP Address
Gateway
IP servers
Option lainnya...

IP1
IP2
IP3

Block Aliran Protocol DHCP



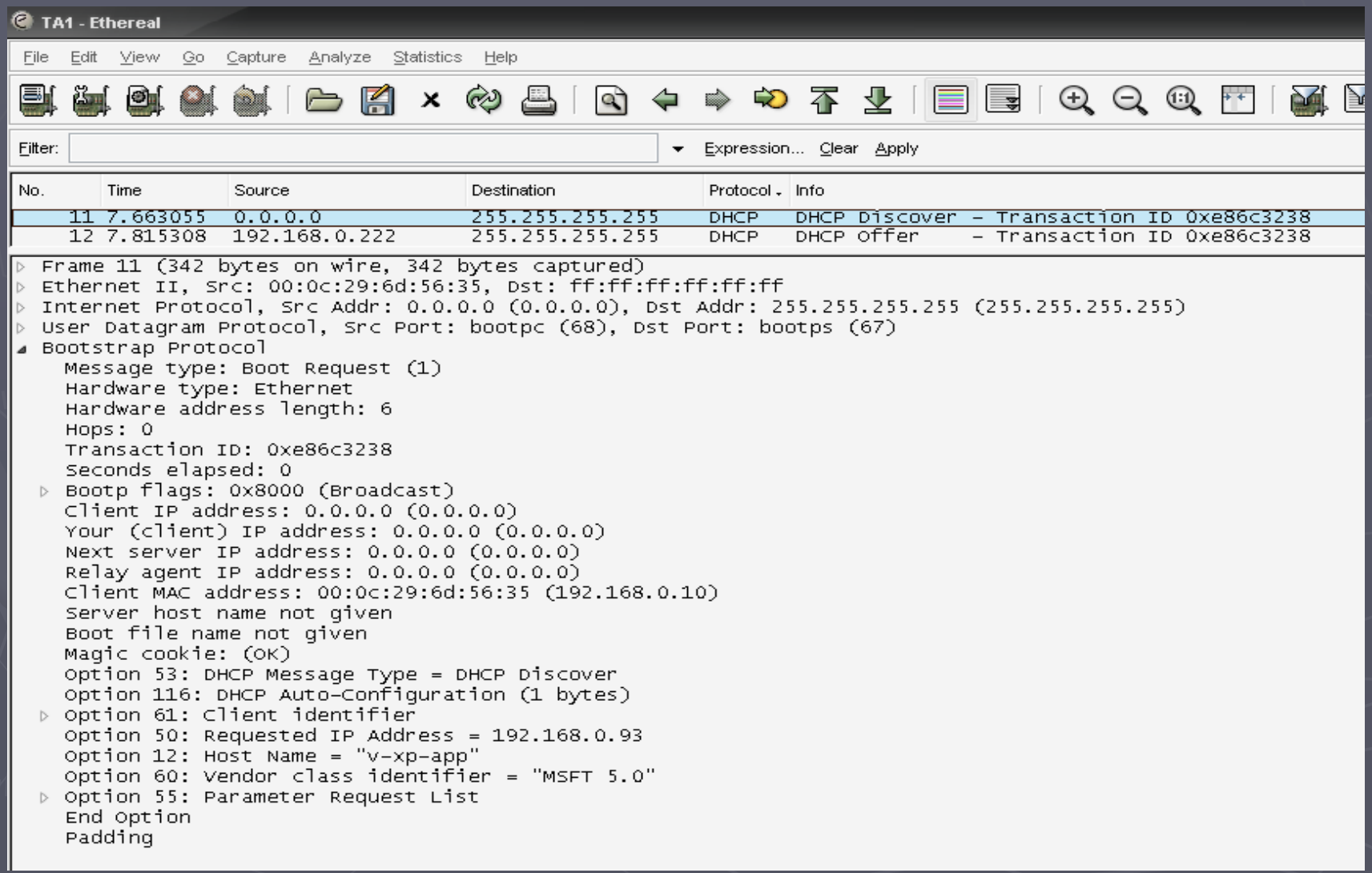
Client State Diagram



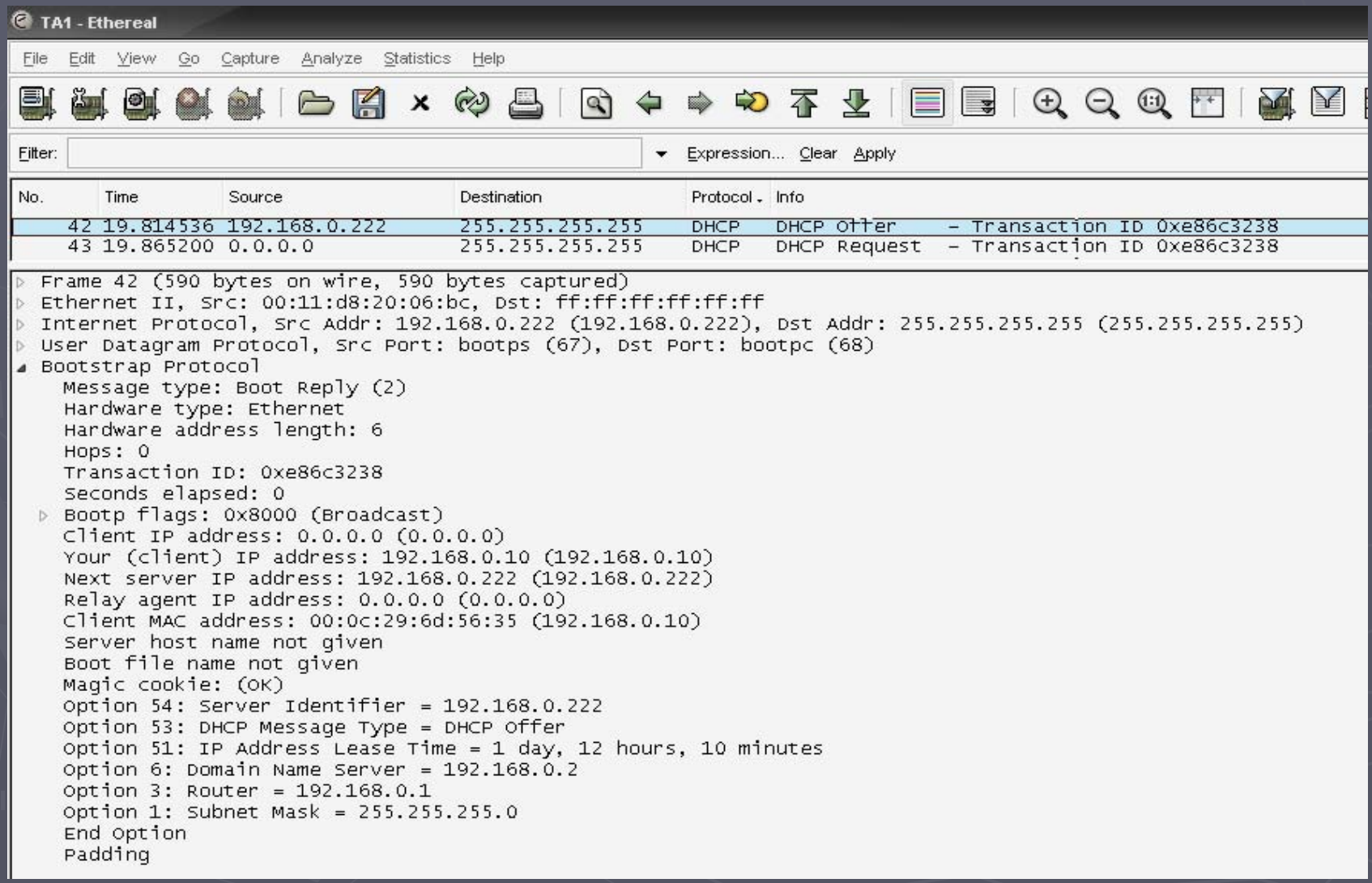
Keterangan

1. Mengirim DHCPREQUEST
2. DHCPNAK/Restart
3. DHCPNAK membuang tawaran
4. DHCPPACK (tidak diterima) / mengirim DHCPDECLINE
5. Mengirim DHCPREQUEST
6. DHCPNAK lease berakhir/ jaringan berhenti
7. memilih tawaran/ mengirim DHCPREQUEST
8. DHCPOFFER /mengumpulkan jawaban
9. DHCPOFFER /membuang
10. DHCPPACK / mencatat lease, mengatur timer T1. T2
11. DHCPACK / mencatat lease, mengatur timer T1, T2
12. DHCPACK/mencatat lease, mengatur timer T1,T2
13. DHCPACK/mencatat lease, mengatur timer T1, T2
14. T1 berakhir /kirim DHCPREQUEST untuk menyewa server
15. T2 berakhir/broadcast DHCP REQUEST
16. DHCPNAK jaringan berhenti

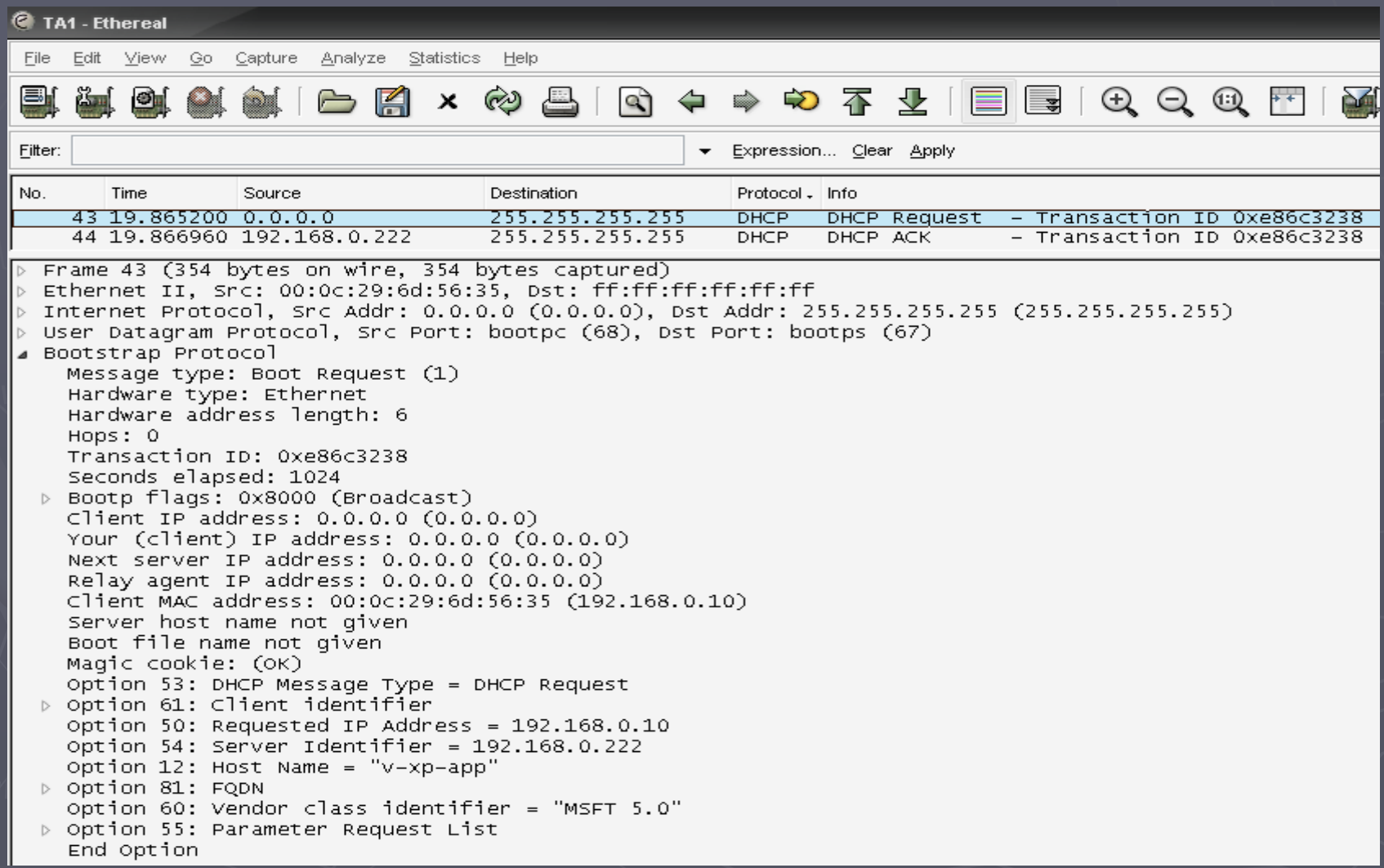
Analisa Packet DHCP (DHCP Discover)



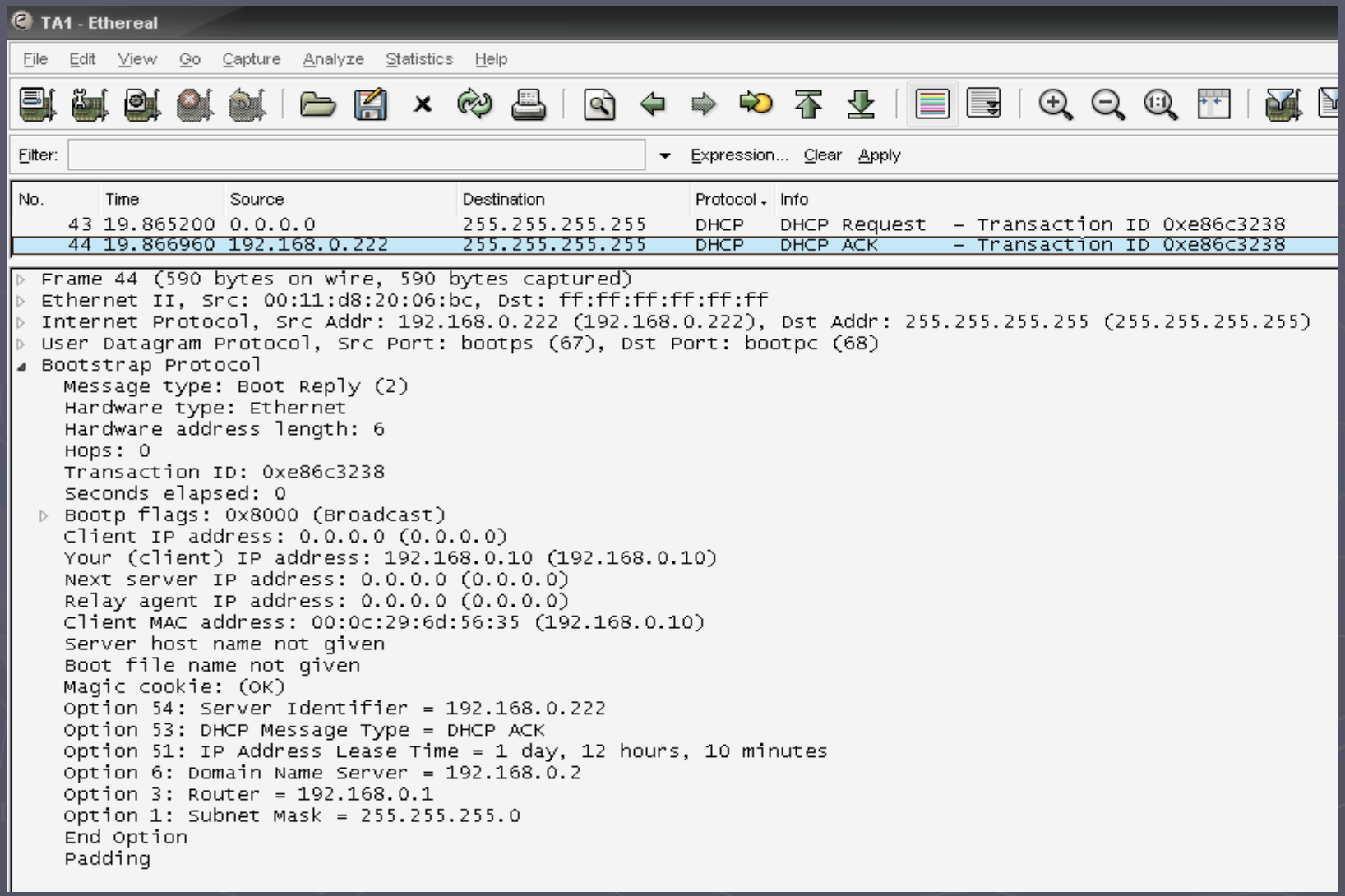
Analisa Packet DHCP (DHCP Offer)



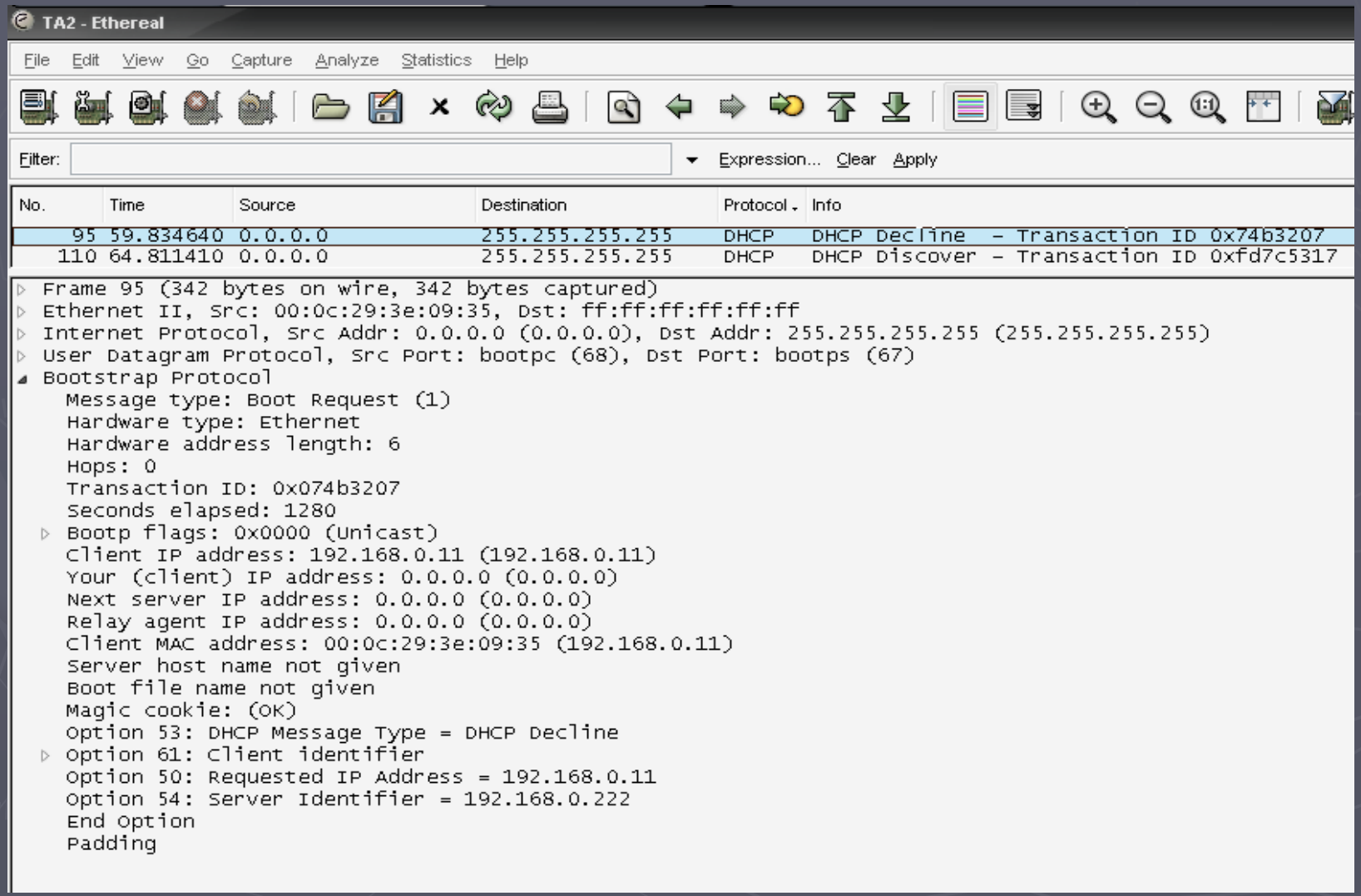
Analisa Packet DHCP (DHCP Request)



Analisa Packet DHCP (DHCP Ack)



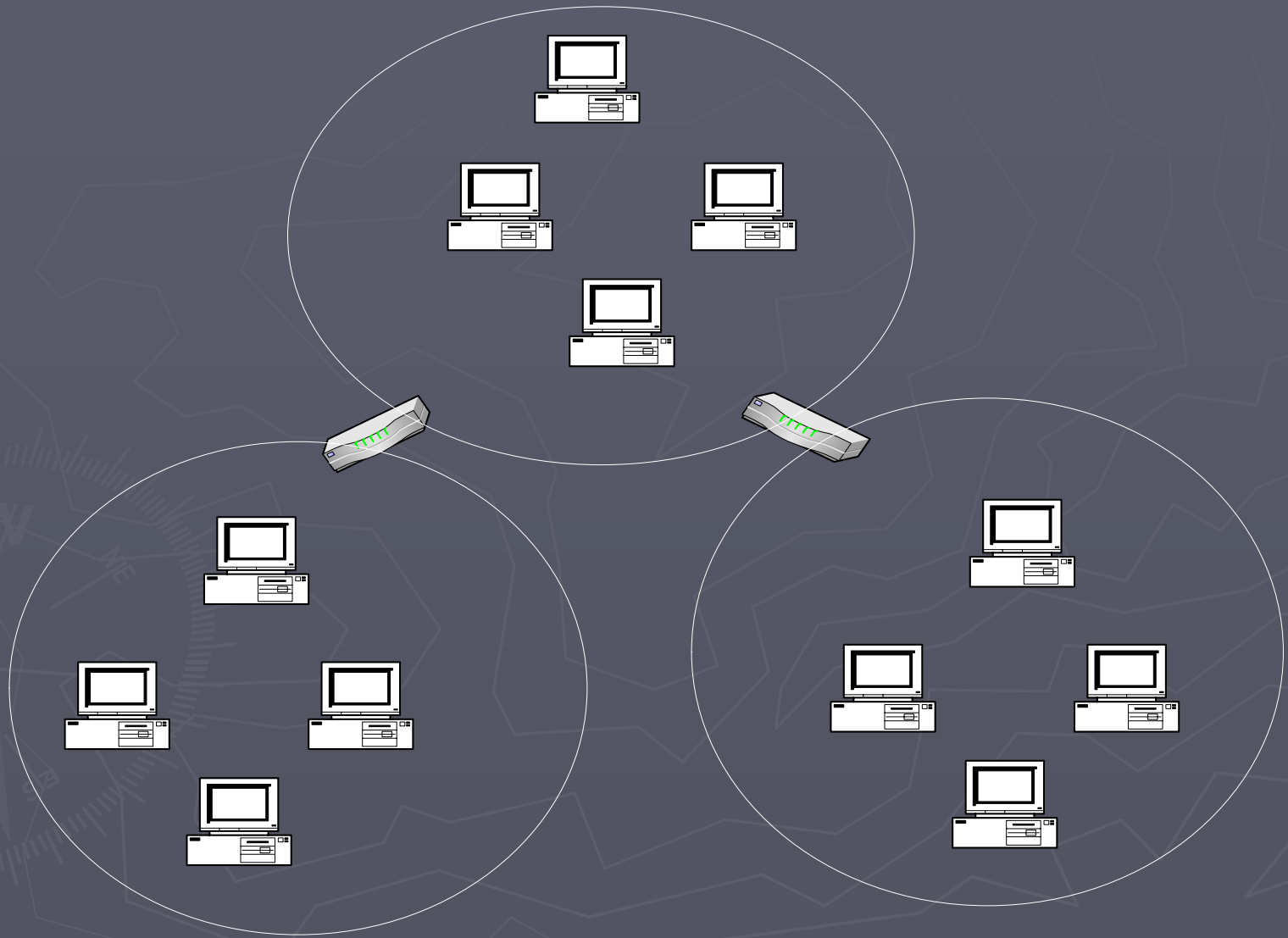
Analisa Packet DHCP (DHCP Decline)



DHCP Relay Agent

- Semua Message DHCP selama proses menggunakan sistem broadcast, hal ini membuat Pesan DHCP tidak sampai pada jaringan yang lain.
- Konsekuensinya perlu diinstall DHCP Relay Agent untuk meneruskan message DHCP diantara jaringan yang ada.
- Router sudah menyiapkan konfigurasi untuk DHCP Relay Agent, baik Cisco Router maupun Server Windows yang berfungsi sebagai router

DHCP Relay Agent



Konfigurasi DHCP server

- File konfigurasi utama DHCP server pada etc/dhcp3/dhcpd.conf

```
option domain-name "test1.com";
option domain-name-servers 192.0.0.1, 194.2.0.50;
option routers 192.0.0.151;
default-lease-time 3600;
subnet 192.0.0.0 netmask 255.255.255.0 {
arrange 192.0.0.200 192.0.0.254;
}
```

Konfigurasi IP Address Statis

```
host hostname {
hardware ethernet 00:B0:CF:8B:49:37;
fixed-address 192.0.0.19;
}
```

Konfigurasi Mesin Client

- # vi /etc/network/interfaces

  auto lo eth0

  iface lo inet loopback

  iface eth0 inet dhcp

- Lakukan restart terhadap konfigurasi jaringan baru

Dynamic DNS

- Kolaborasi antara DNS dan DHCP
- Membutuhkan bind9 dan DHCP3
- Konfigurasi file utama : dhcpd.conf dan named.conf

```
# /etc/dhcp/dhcpd.conf
########################################################################

server-identifier zenith.example.com;
authoritative;
# this is the most important line. It specifies the method
# to use to connect to the DNS server and update it.
ddns-update-style interim;

# this has to be the same key as is used in named.conf
key mykey {
algorithm hmac-md5;
secret "secret_md5_hash";
};
# this section describes what key to use in what zone
zone example.com. {
primary 192.168.0.9;
key mykey;
}
zone 0.168.192.in-addr.arpa. {
primary 192.168.0.9;
key mykey;
}
# and this section holds all the options for the subnet listed,
# including the range of addresses to lease out, gateways etc.
subnet 192.168.0.0 netmask 255.255.255.0 {
  # use these addresses:
  range 192.168.0.10 192.168.0.20;
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.168.0.255;
  option domain-name "example.com";
  one-lease-per-client on;
  default-lease-time 14400;
  max-lease-time 14401;
  option ip-forwarding off;
  option time-offset -18000;
  # set a few handy default options
  option routers 192.168.0.9;
  option domain-name-servers 192.168.0.9;
  option smtp-server 192.168.0.9;
  option netbios-name-servers 192.168.0.9;
}
```

```
////////////////////////////////////////////////////////////////////////
// /etc/bind/named.conf
////////////////////////////////////////////////////////////////////////

// First off is the key. To modify the running DNS server you need
// this, the same as in the dhcpd.conf file.
key mykey {
  algorithm hmac-md5;
  secret "secret_md5_hash";
};
// Next the access control section, we allow the 192.168.0.0-255
// subnet, and localhost.
acl "home" { 192.168.0.0/24; 127.0.0.1;};
// Some general options, including who to forward queries you can't
// resolve to. (in this case they are claranet's dns servers.)
options {
  directory "/var/bind/"; //Working directory
  pid-file "/var/run/named/named.pid";
  allow-query { "home"; };
  forwarders { 195.8.69.7; 195.8.69.12; };
};
// You need this section to allow the communication between
// daemons. (dhcp and bind)
controls {
  inet 127.0.0.1 port 953
  allow { 127.0.0.1; 192.168.0.9; } keys { "mykey";
};
};
// And then you have pretty much standard zones, except for the
// fact that the key specified at the top is allowed to modify the
// domain zone and reverse zone at the bottom.
zone "0.0.127.in-addr.arpa" {
  type master;
  file "localhost.rev";
  notify no;
};
zone "example.com" {
  type master;
  notify no;
  file "/var/bind/example.com";
  allow-update { key mykey; };
};
zone "0.168.192.in-addr.arpa"{
  type master;
  notify no;
  file "/var/bind/example.com.rev";
  allow-update { key mykey; };
};
zone "." {
  type hint;
  file "named.ca";
};
////////////////////////////////////////////////////////////////////////
```

Zone Files

```
;
; SOA: Start of authority record - this NS is the best source of info in this
; zone (See DNS and Bind book, ch 4.)
;
$ORIGIN .
$TTL 86400  ; 1 day
example.com.IN SOAexample.com. nadir.example.com. (
2000111383 ; serial
10800      ; refresh (3 hours)
3600       ; retry (1 hour)
604800      ; expire (1 week)
86400      ; minimum (1 day)
)
;
; Name servers: same domain name as origin.
;
IN NSnadir.example.com.

;
; Name to address mappings follow. Address to name mappings can be found in
; home.hosts.rev
;
; Put any addresses you want fixed here. Dynamically set addresses will appear
; below.
;
nadir.example.comIN A192.168.0.254
```

Reverse Zone

```
;
; SOA section: like above only maps addresses to names.
;
$ORIGIN .
$TTL 86400  ; 1 day
0.168.192.in-addr.arpaIN SOAexample.com. nadir.example.com. (
2000107274 ; serial
28800      ; refresh (8 hours)
14400      ; retry (4 hours)
3024000    ; expire (5 weeks)
86400      ; minimum (1 day)
)
;
; Name Servers
;
IN NSnadir.example.com.

;
; Fixed addresses, followed by DDNS inserted mappings.
;
254.0.168.192.in-addr.arpa. PTR nadir.example.com.
```

Troubleshooting

- Cek apakah BIND mempunyai hak menulis pada /var/bind.
- DHCP Client harus mengirimkan hostname-nya
  - send host-name "hostname"