Network Layer

MUHAMMAD ZEN S. HADI, ST. MSC.

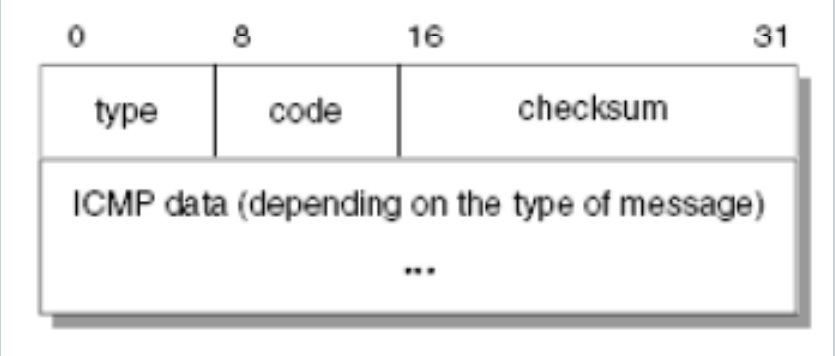
Topik

- Protokol lapisan network
  (ARP, RARP, DHCP, ICMP)
- Aplikasi (arp, ping, tracert, nbtstat)

Internet Control Message Protocol (ICMP)

- Karakterisitk dari ICMP
  - ICMP menggunakan IP
  - ICMP melaporkan kerusakan
  - ICMP tidak akan merespon kepada IP datagram yang tidak memiliki header IP pengirim

Format Pesan ICMP



- Jenis Pesan :

  a. Echo reply dan echo request

  b. Destination unreachable

  c. Time exceeded

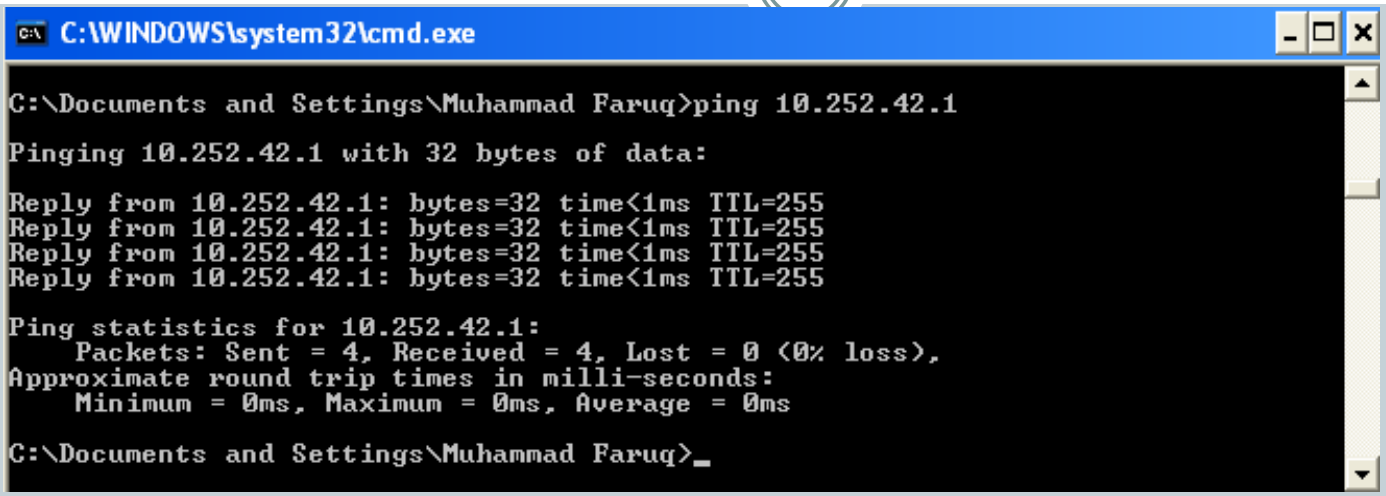
  d. Dll

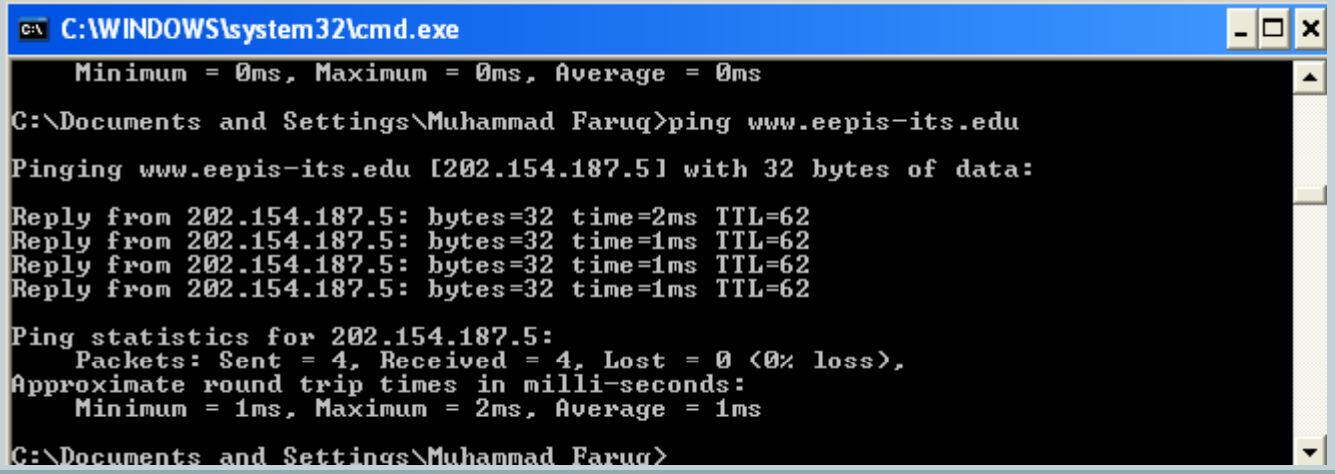
Aplikasi ICMP

- PING (Packet InterNet Groper)

  Ping mengirimkan IP datagram ke suatu host dan mengukur waktu round trip dan menerima respon.
- Ping menggunakan pesan ICMP echo request dan echo reply.

Contoh PING

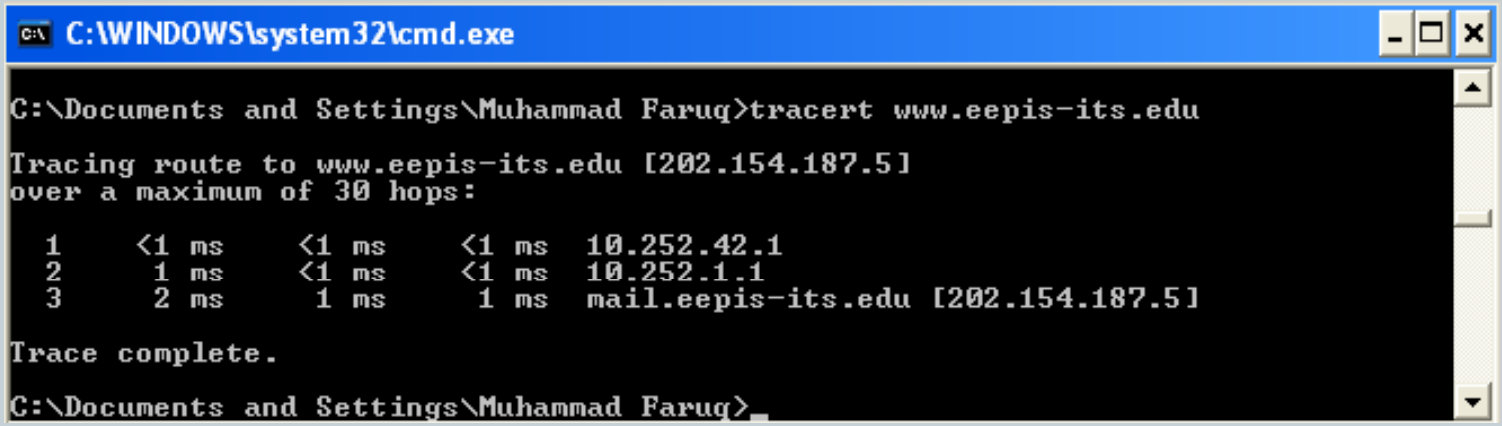

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Muhammad Faruq>ping 10.252.42.1
Pinging 10.252.42.1 with 32 bytes of data:
Reply from 10.252.42.1: bytes=32 time<1ms TTL=255
Reply from 10.252.42.1: bytes=32 time<1ms TTL=255
Reply from 10.252.42.1: bytes=32 time<1ms TTL=255
Reply from 10.252.42.1: bytes=32 time<1ms TTL=255
Ping statistics for 10.252.42.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Documents and Settings\Muhammad Faruq>_


C:\WINDOWS\system32\cmd.exe
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Documents and Settings\Muhammad Faruq>ping www.eepis-its.edu
Pinging www.eepis-its.edu [202.154.187.5] with 32 bytes of data:
Reply from 202.154.187.5: bytes=32 time=2ms TTL=62
Reply from 202.154.187.5: bytes=32 time=1ms TTL=62
Reply from 202.154.187.5: bytes=32 time=1ms TTL=62
Reply from 202.154.187.5: bytes=32 time=1ms TTL=62
Ping statistics for 202.154.187.5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\Documents and Settings\Muhammad Faruq>

APLIKASI ICMP

- Traceroute

  Aplikasi traceroute melacak jalur mana saja yang dilalui untuk menuju ke suatu host tujuan.



ARP

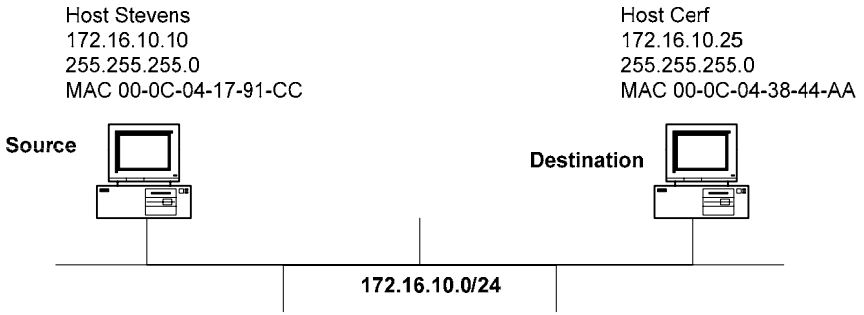
- ARP kepanjangan dari Address Resolution Protocol, suatu protokol yang bertugas mengolah pengalamatan logik dan fisik jaringan
- ARP mengolah sebuah tabel yang berisi Mapping antara IP-address dan Ethernet Card.
- Tabel arp didapatkan dari request (broadcast) ke jaringan.
- Berada pada layer 3 Jaringan

ARP Table

IP Address	MAC Address
172.16.10.3	00-0C-04-32-14-A1
172.16.10.19	00-0C-14-02-00-19
172.16.10.33	00-0C-A6-19-46-C1

Mengapa Butuh Mapping MAC Address dengan IP Address

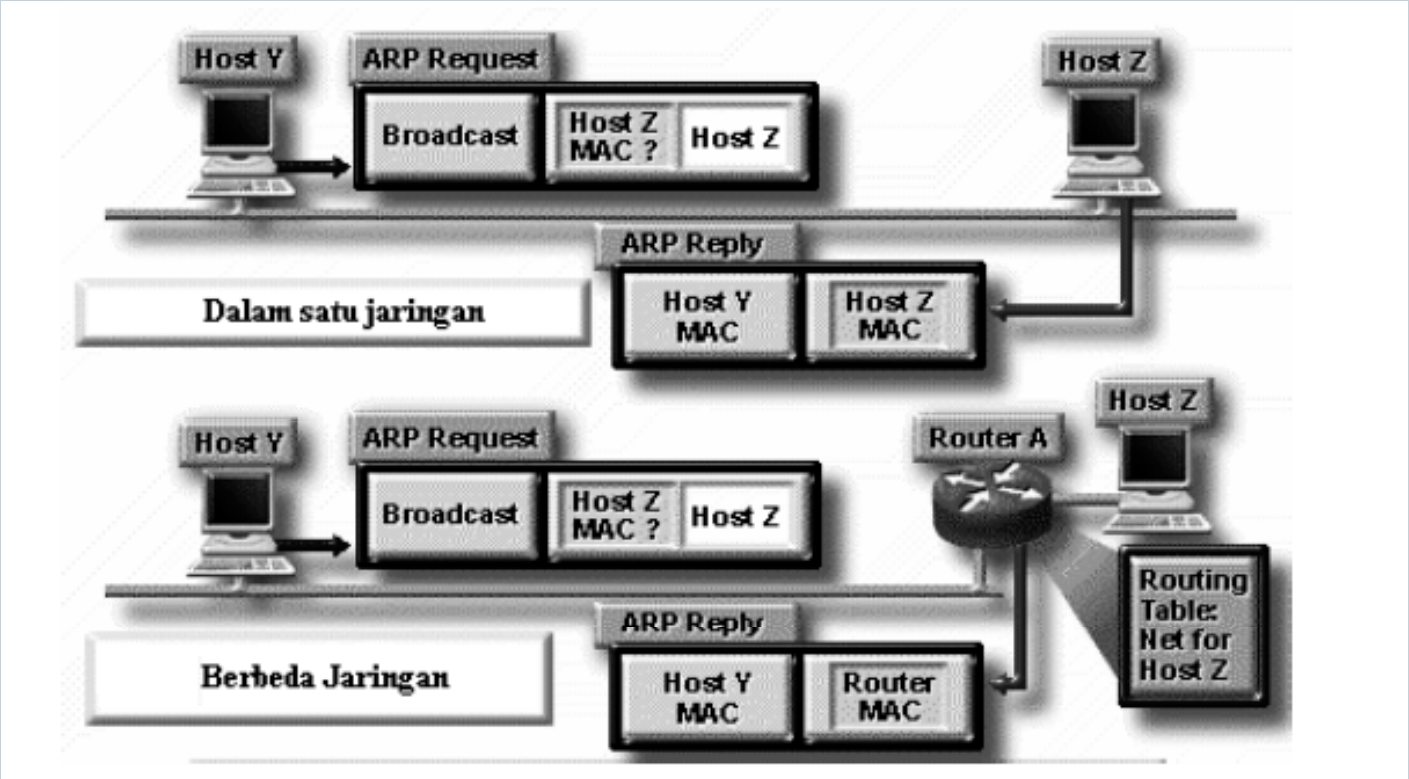
- Jika host ingin berkomunikasi IP host tertentu, Komputer sumber akan melakukan pengecekan nomor MAC dari komputer tujuan di Tabel ARP
- Jika di tabel ARP tidak ditemukan, maka melakukan arp request



Data link destination address	Data link source address	Other data link fields
???	00-0C-04-17-91-CC	

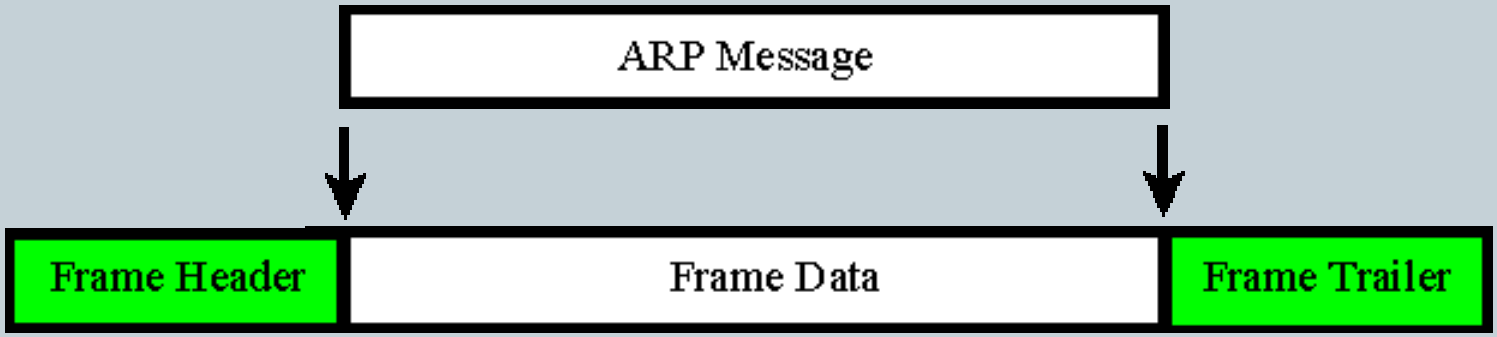
IP Destination Address	IP Source Address	Other IP fields and data
172.16.10.25	172.16.10.10	

Cara Kerja protokol ARP



ARP Request

Ethernet Header			**Ethernet Data – 28 byte ARP request/reply**				
Ethernet Destination Address (MAC)	Ethernet Source Address (MAC)	Frame Type	ARP headers , i.e. op field	Sender's Ethernet Address (MAC)	Sender's IP Address	Target's Ethernet Address (MAC)	Target's IP Address



NBTSTAT

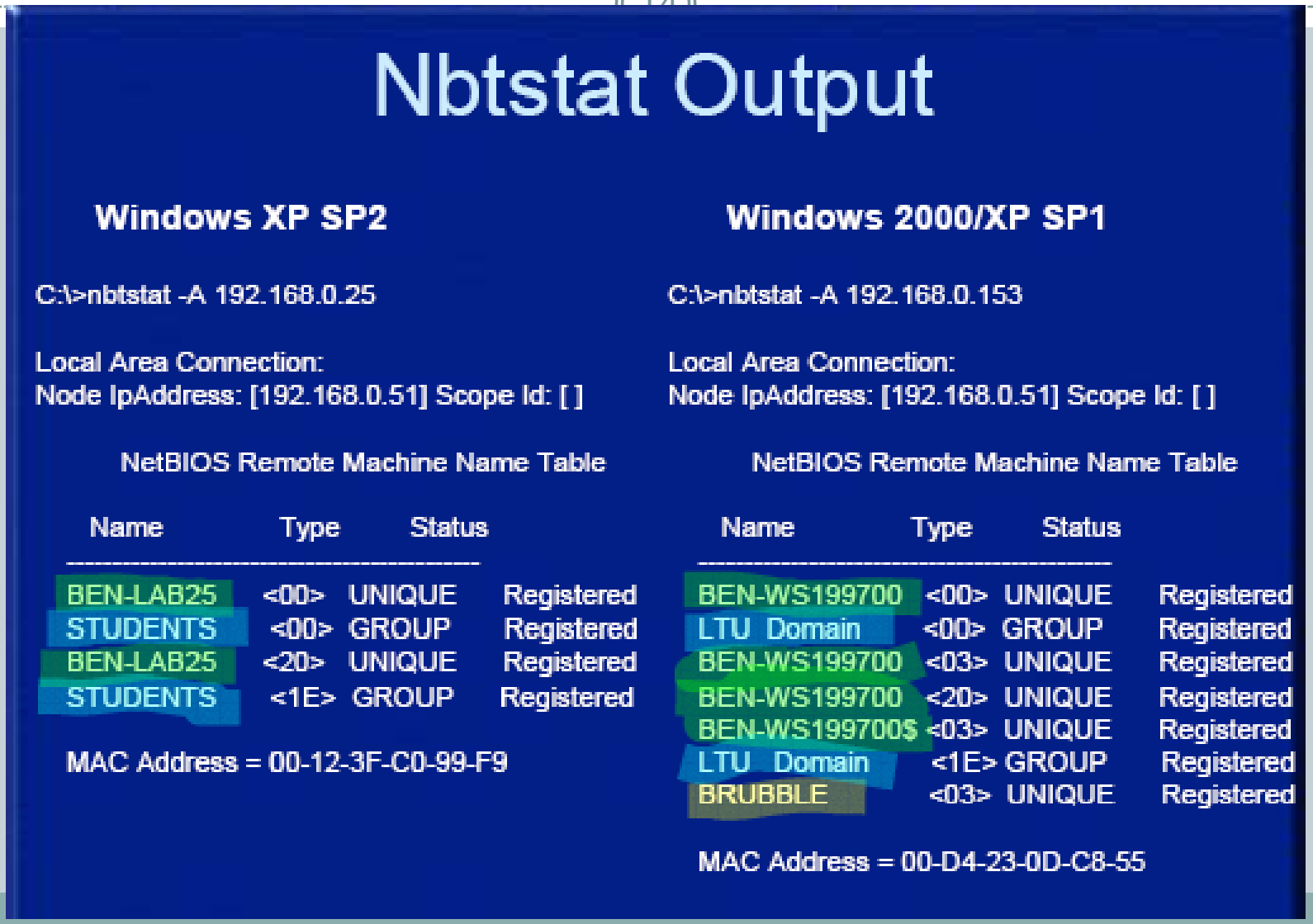
- Berbasis Windows

  Menampilkan statistik protokol, tabel nama dan koneksi TCP/IP saat ini menggunakan NBT (NetBIOS over TCP/IP)
- Built-in dalam sistem operasi Windows

Hostname Resolution: NetBIOS name query


```
C:\>ping tyrell

Pinging tyrell [192.168.1.103] with 32 bytes of data:

Reply from 192.168.1.103: bytes=32 time<10ms TTL=255
Reply from 192.168.1.103: bytes=32 time<10ms TTL=255
Reply from 192.168.1.103: bytes=32 time<10ms TTL=255
Reply from 192.168.1.103: bytes=32 time<10ms TTL=255

Ping statistics for 192.168.1.103:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>nbtstat -c

Local Area Connection:
Node IpAddress: [192.168.1.100] Scope Id: []

                NetBIOS Remote Cache Name Table

       Name              Type       Host Address    Life [sec]
    --------------------------------------------------------
    TYRELL         <00>  UNIQUE          192.168.1.103       592

C:\>arp -a

Interface: 192.168.1.100 on Interface 0x1000003
  Internet Address      Physical Address      Type
  192.168.1.103         00-50-da-70-1e-24     dynamic
```

Nbtstat Output



Dynamic Host Configuration protocol

Pendahuluan

- Kepanjangan dari Dynamic Host Configuration Protocol
- Merupakan protokol yang dipakai untuk memberikan IP secara dinamis kepada client yang tidak mempunyai nomor IP
- Standarisasi :
  - RFC 2131: Dynamic Host Configuration Protocol
  - RFC 2132: DHCP Options and BOOTP Vendor Extensions
- Beberapa informasi yang bisa dikirim bersama nomor IP
  - IP dan default router/gateway
  - Name Server
  - File Server, dll
- Sebagai Pengendalian parameter bagi komputer client, sehingga admin tidak perlu konfigurasi tiap komputer

Pendahuluan...

- Persyaratan DHCP Server :
  - Host-host yang terkonfigurasi secara statis bisa berdampingan dengan yang dinamis menggunakan DHCP Server
  - Jaminan alamat unique
  - Menjaga informasi client
  - Jika client booting sedapatkan mungkin diberi IP yang sama
- Merupakan perbaikan dari Bootstrap Protocol (BOOTP)

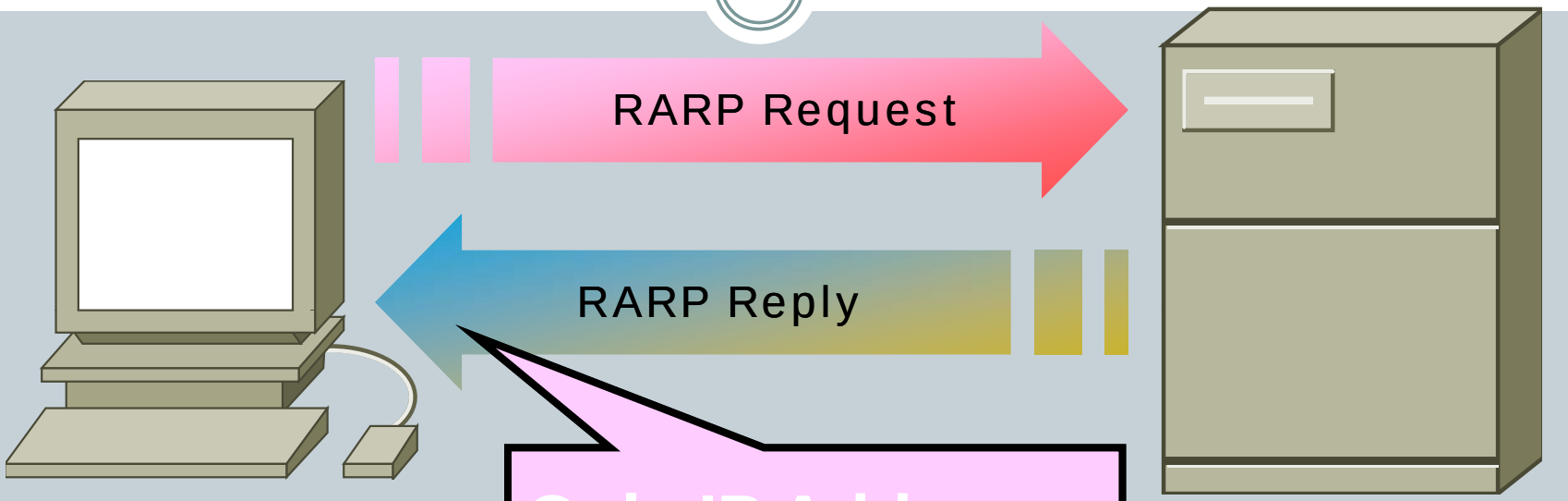
Kenapa Butuh DHCP Server ?

- 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

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

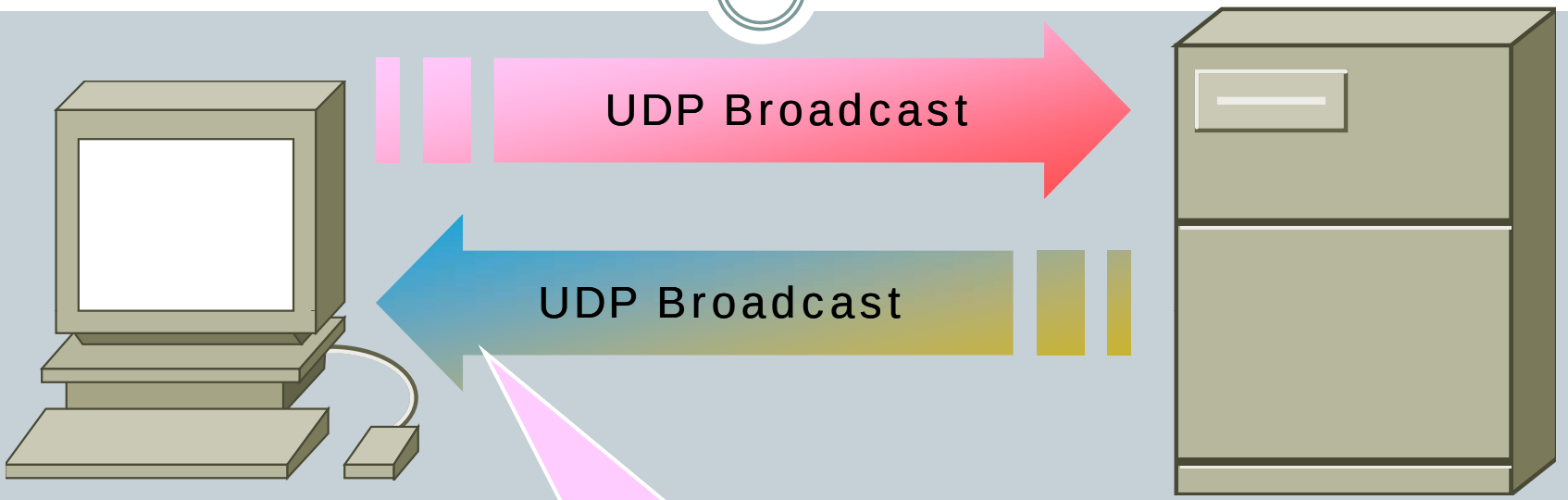


MAC HEADER	IP HEADER	RARP REQUEST MESSAGE
Destination 08-00-02-89-90-8 Source 02-60-8C-01-02-03	Destination 11111111 Source ????????	What is my IP address?

BOOTP

- Merupakan protokol yang dipakai sebelum DHCP
- Yang dapat dilakukan oleh BOOTP :
  - Pemberian nomor IP, Default Gateway dan Netmask
  - Dapat digunakan untuk download image untuk diskless sistem
  - IP yang diberikan statis tidak pernah berubah
- Dikirim menggunakan Protokol UDP pada port 67 pada server dan port 68 pada client

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

Format Paket DHCP

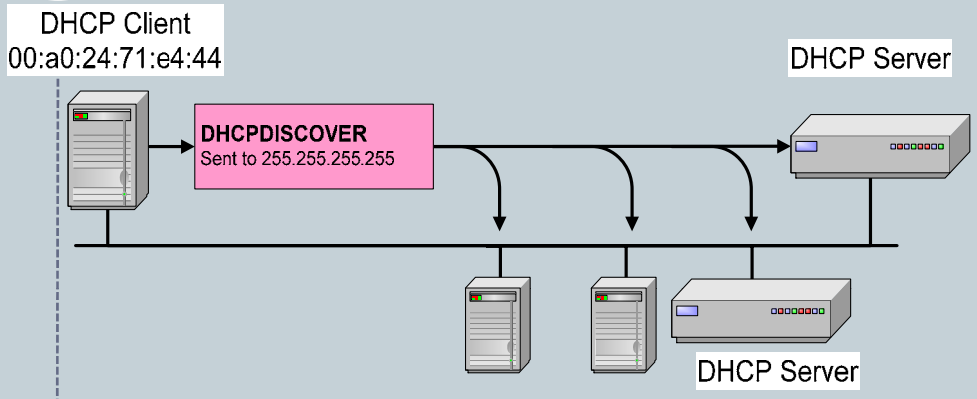
- Ide dasar memberikan IP ke client, server harus ingat IP tersebut dan parameternya.
- Yang dikirim bukan Cuma IP tapi juga parameter - parameter
- Jika client booting sedapatkan mungkin diberi IP yang sama.

Aturan dan Proses RFC 2131

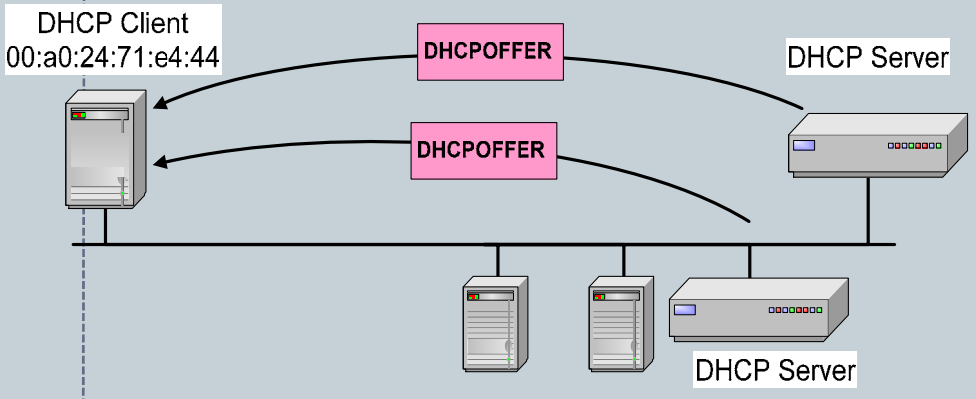
- Ketika DHCP client masuk/bergabung kedalam suatu jaringan, client tesebut akan melakukan broadcast dengan mengirimkan pesan DHCPDISCOVER ke suatu network.
- Seluruh DHCP server akan merespon DHCPDISCOVER yang dikirimkan DHCP client tersebut dengan DHCPOFFER.
- Ketika client mendapatkan DHCPOFFER, client 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

DHCP Operation

- DCHP DISCOVER

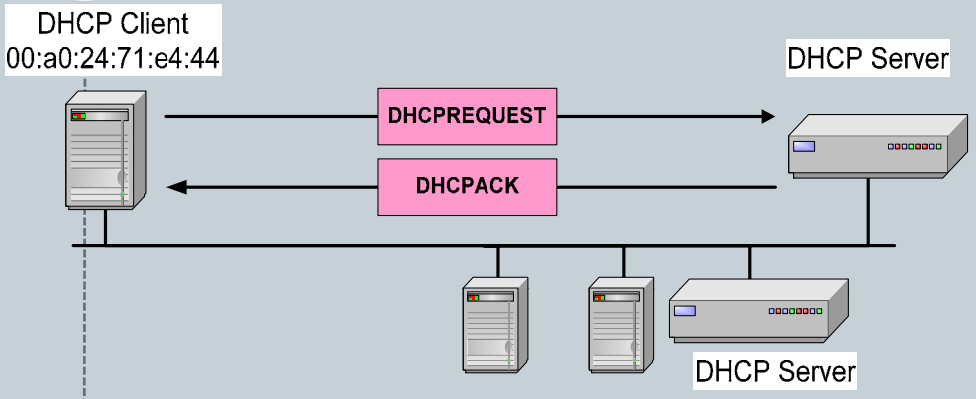


- DCHP OFFER

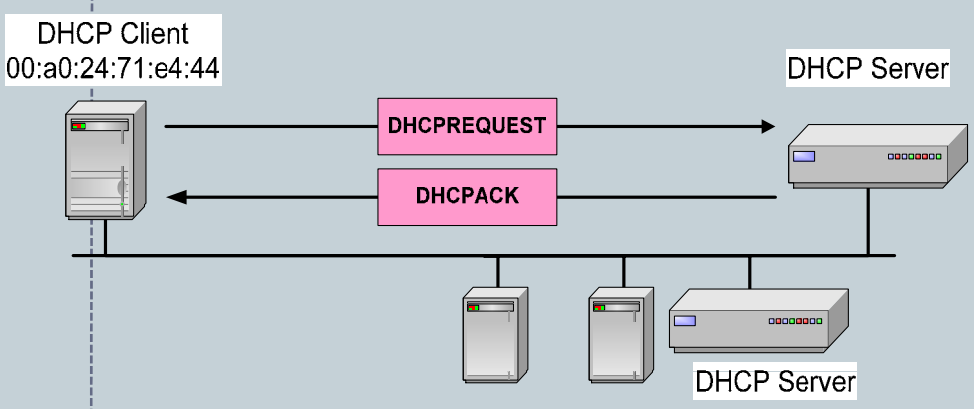


DHCP Operation

- DCHP REQUEST

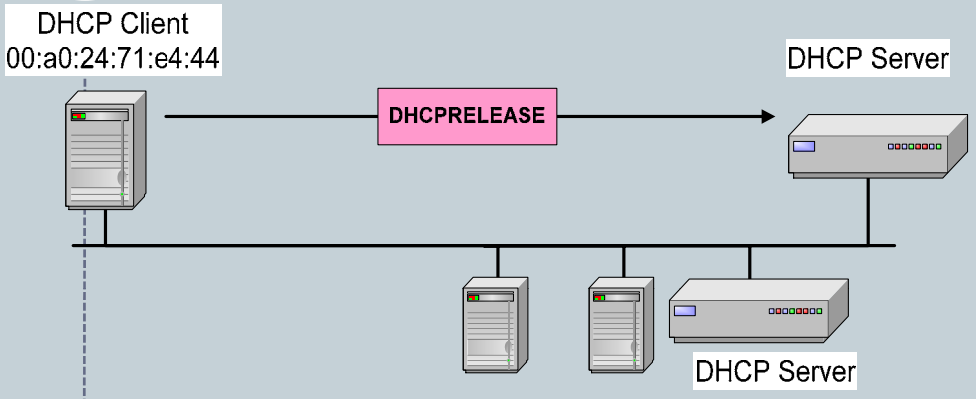


- DCHP ACK

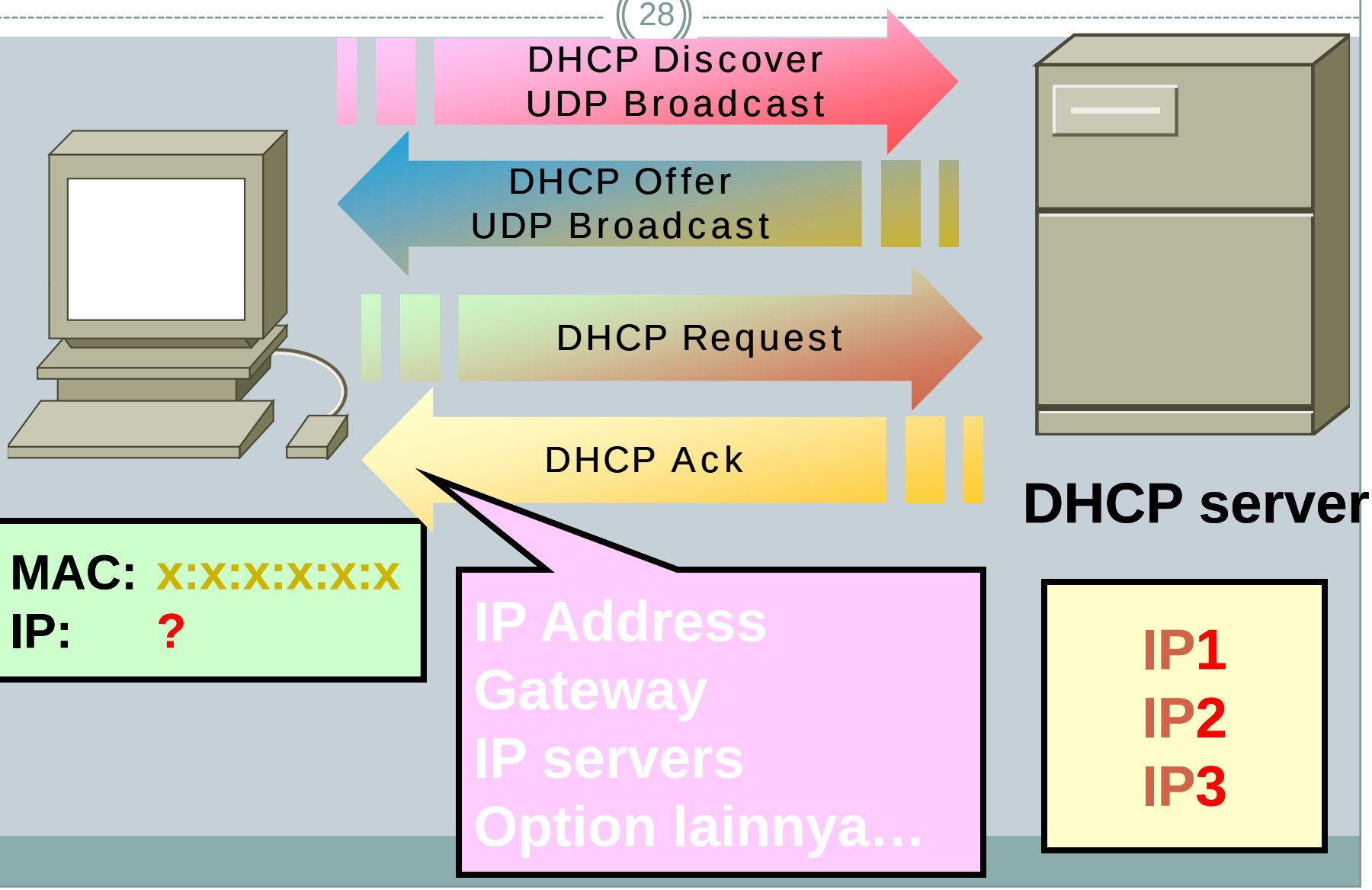


DHCP Operation

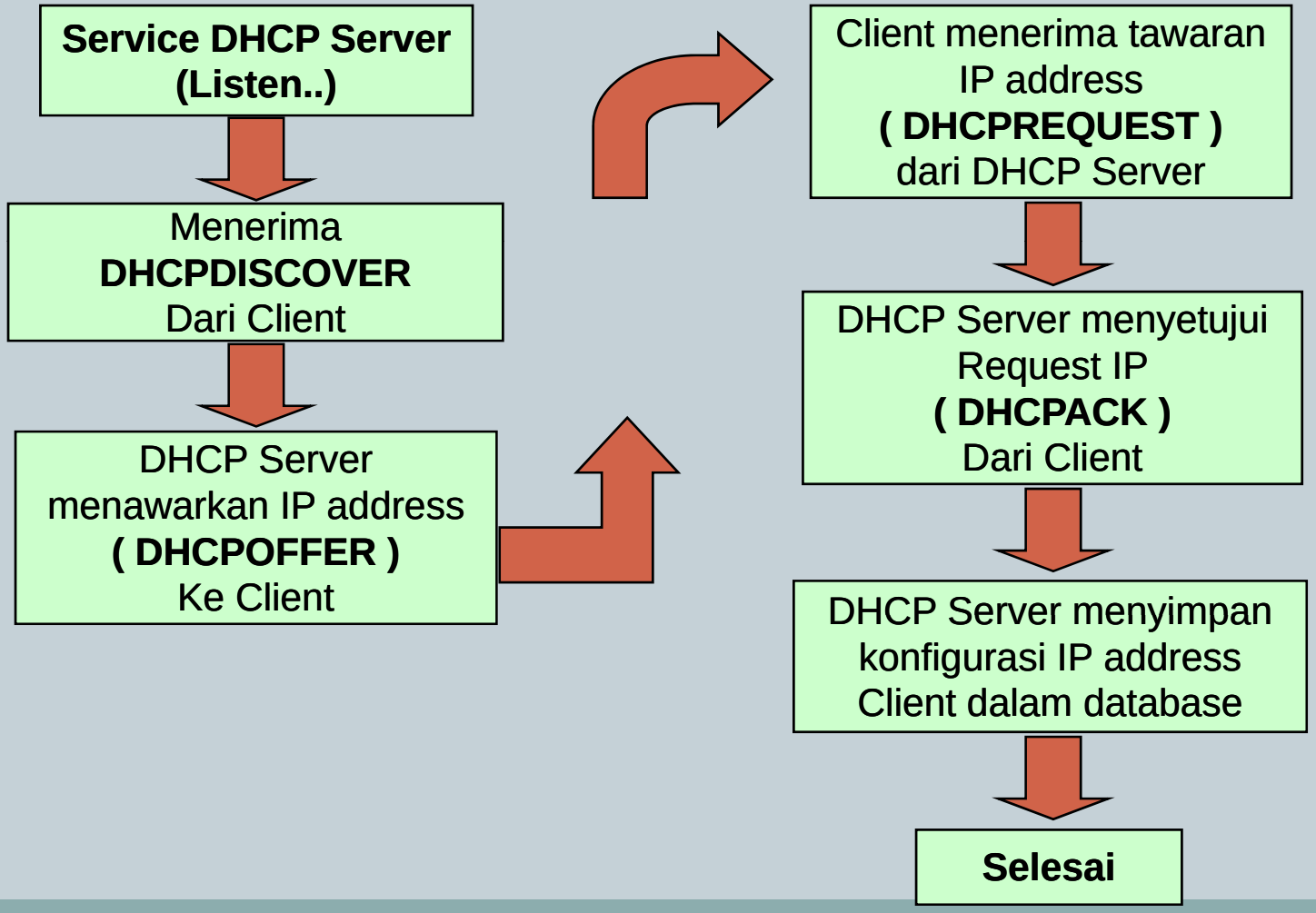
- DCHP RELEASE



Sistem Kerja DHCP



Block Aliran Protocol DHCP



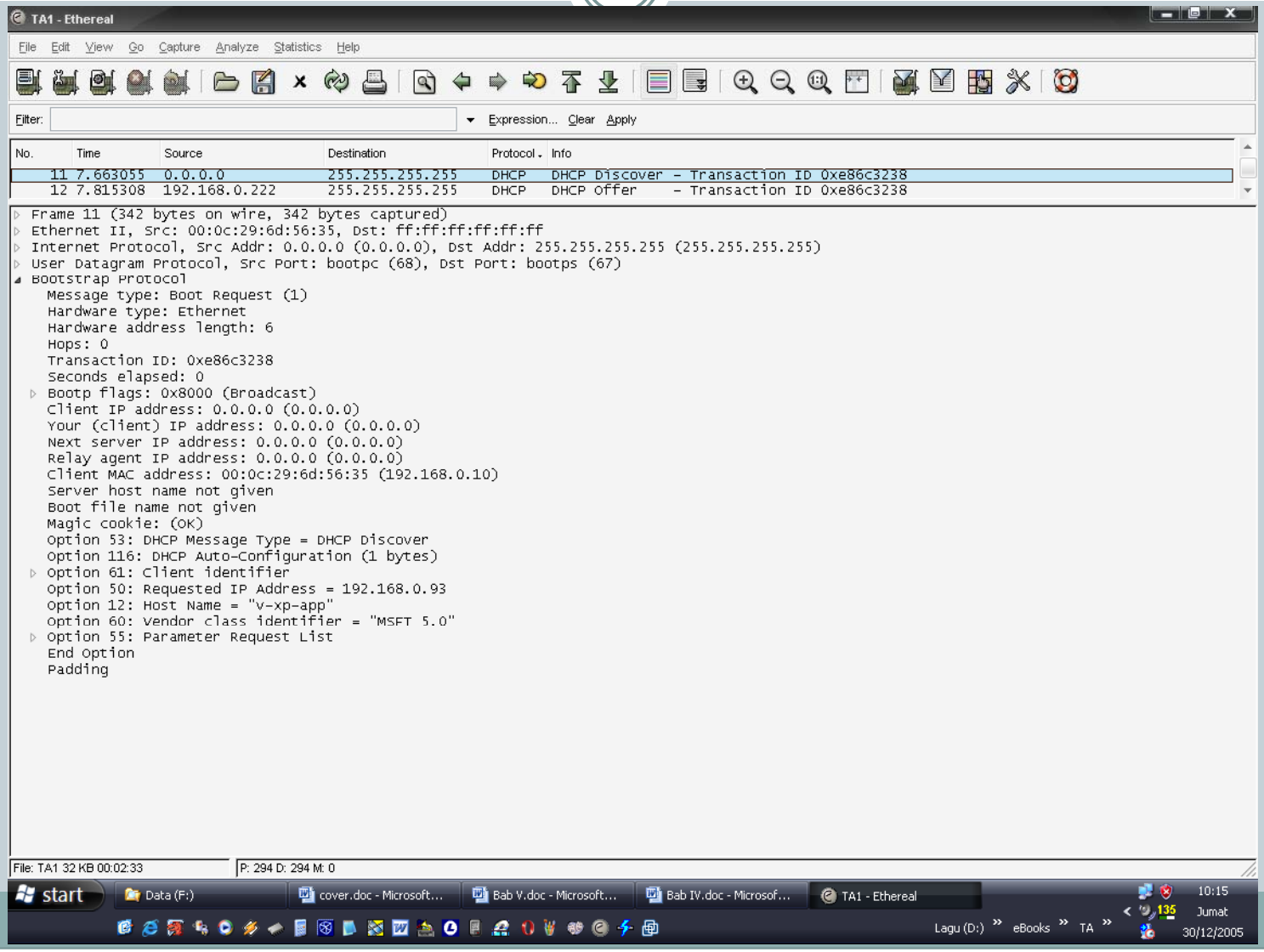
DHCP Message

- 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’

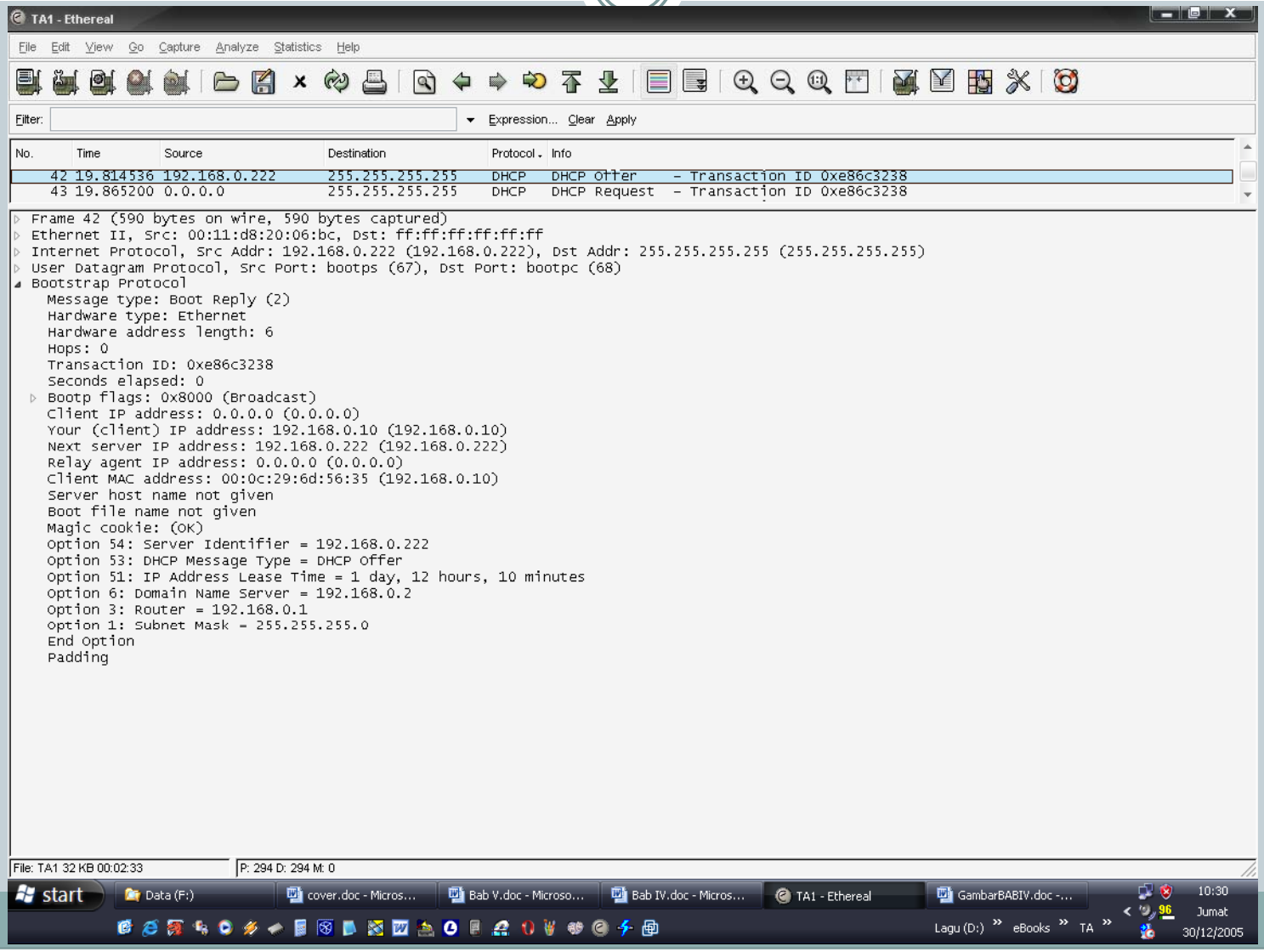
DHCP Message

- 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'.

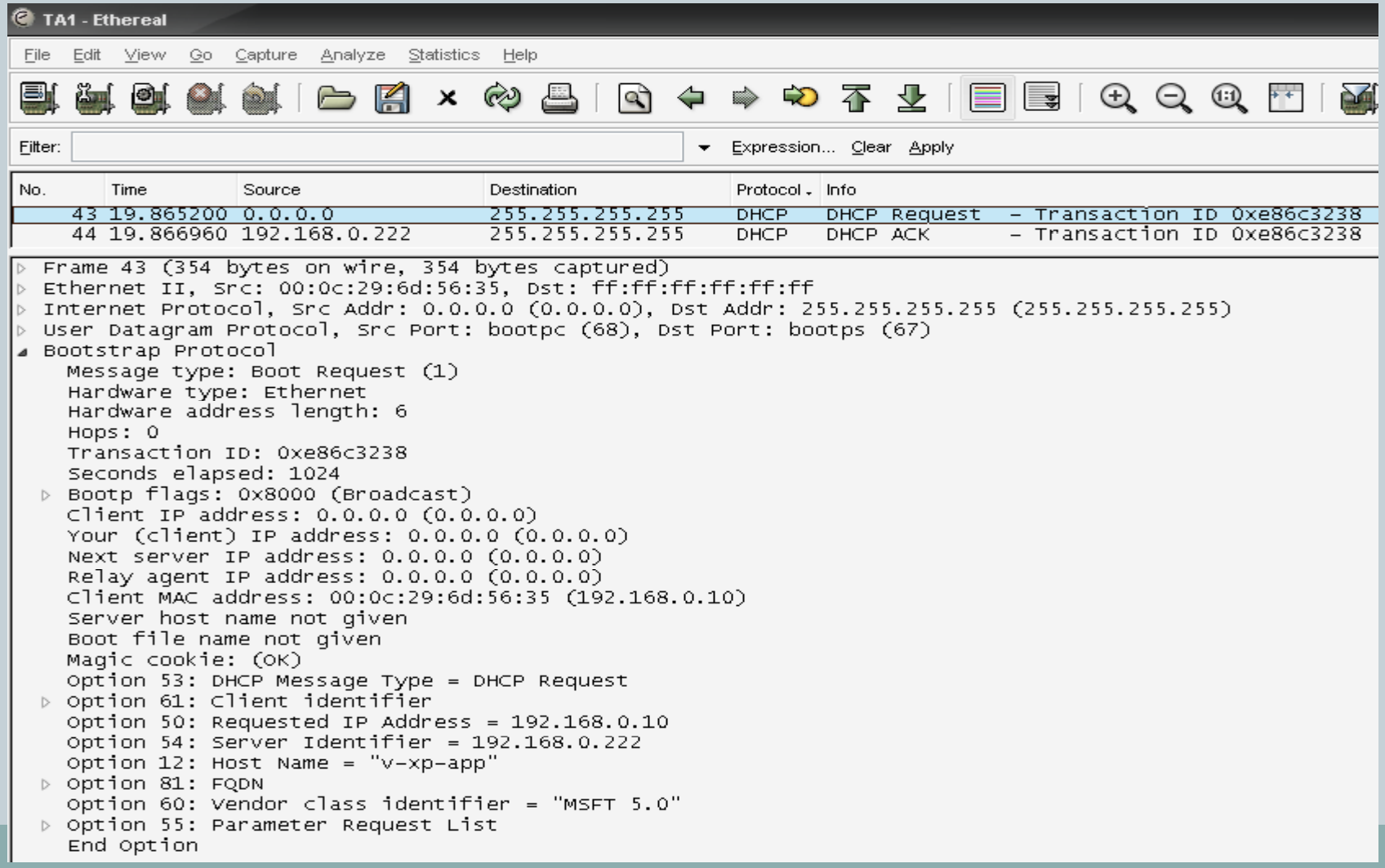
Analisa Packet DHCP (DHCP Discover)



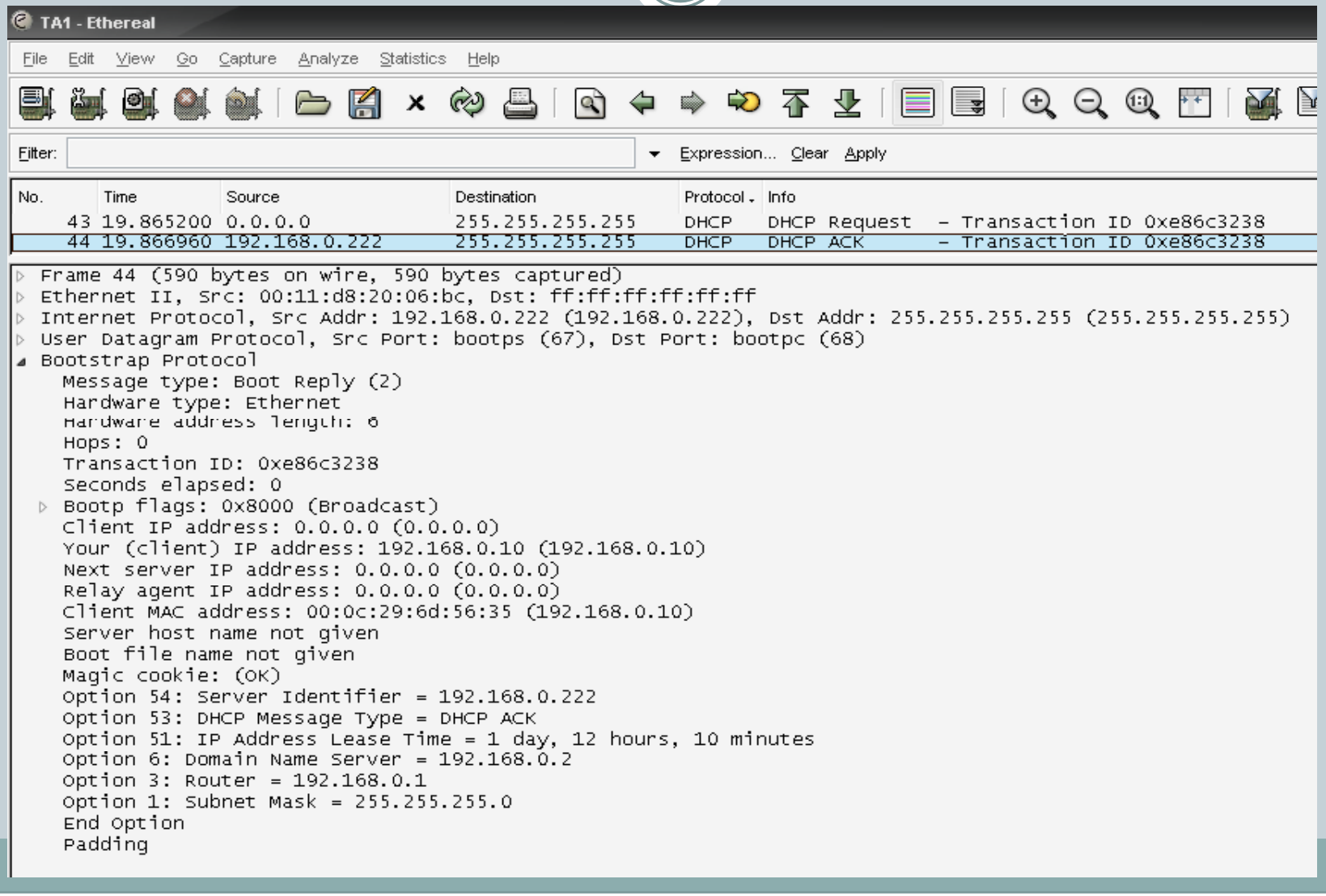
Analisa Packet DHCP (DHCP Offer)



Analisa Packet DHCP (DHCP Request)



Analisa Packet DHCP (DHCP Ack)



Analisa Packet DHCP (DHCP Decline)