

Network Layer

1

MUHAMMAD ZEN S. HADI, ST. MSC.

Topik

2

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

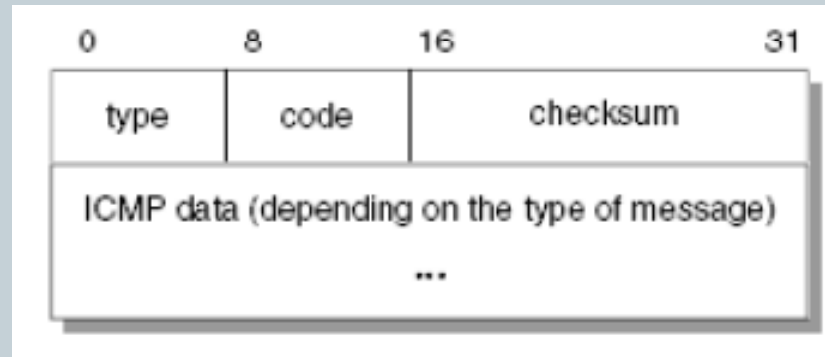
Internet Control Message Protocol (ICMP)

3

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

Format Pesan ICMP

4



- **Jenis Pesan :**
 - a. Echo reply dan echo request
 - b. Destination unreachable
 - c. Time exceeded
 - d. Dll

Aplikasi ICMP

5

- 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

6

```
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>_
```

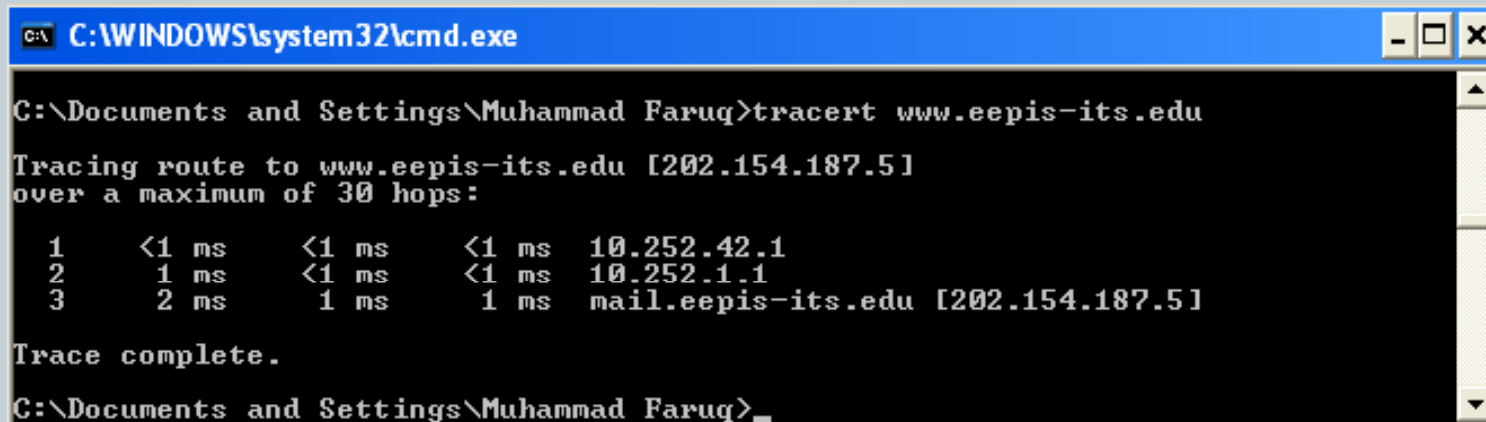
```
C:\WINDOWS\system32\cmd.exe
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Documents and Settings\Muhammad Faruq>ping www.eepis-its.edu
Pinging www.eepis-its.edu [202.154.187.5] with 32 bytes of data:
Reply from 202.154.187.5: bytes=32 time=2ms TTL=62
Reply from 202.154.187.5: bytes=32 time=1ms TTL=62
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

7

- Traceroute

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



```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Muhammad Faruq>tracert www.eepis-its.edu

Tracing route to www.eepis-its.edu [202.154.187.5]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms    10.252.42.1
  2     1 ms     <1 ms    <1 ms    10.252.1.1
  3     2 ms     1 ms     1 ms    mail.eepis-its.edu [202.154.187.5]

Trace complete.

C:\Documents and Settings\Muhammad Faruq>
```

ARP

8

- 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

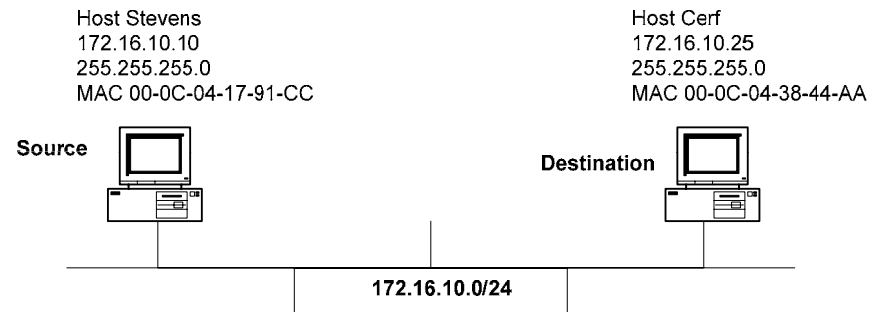
ARP Table

<u>IP Address</u>	<u>MAC Address</u>
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

9

- 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

???

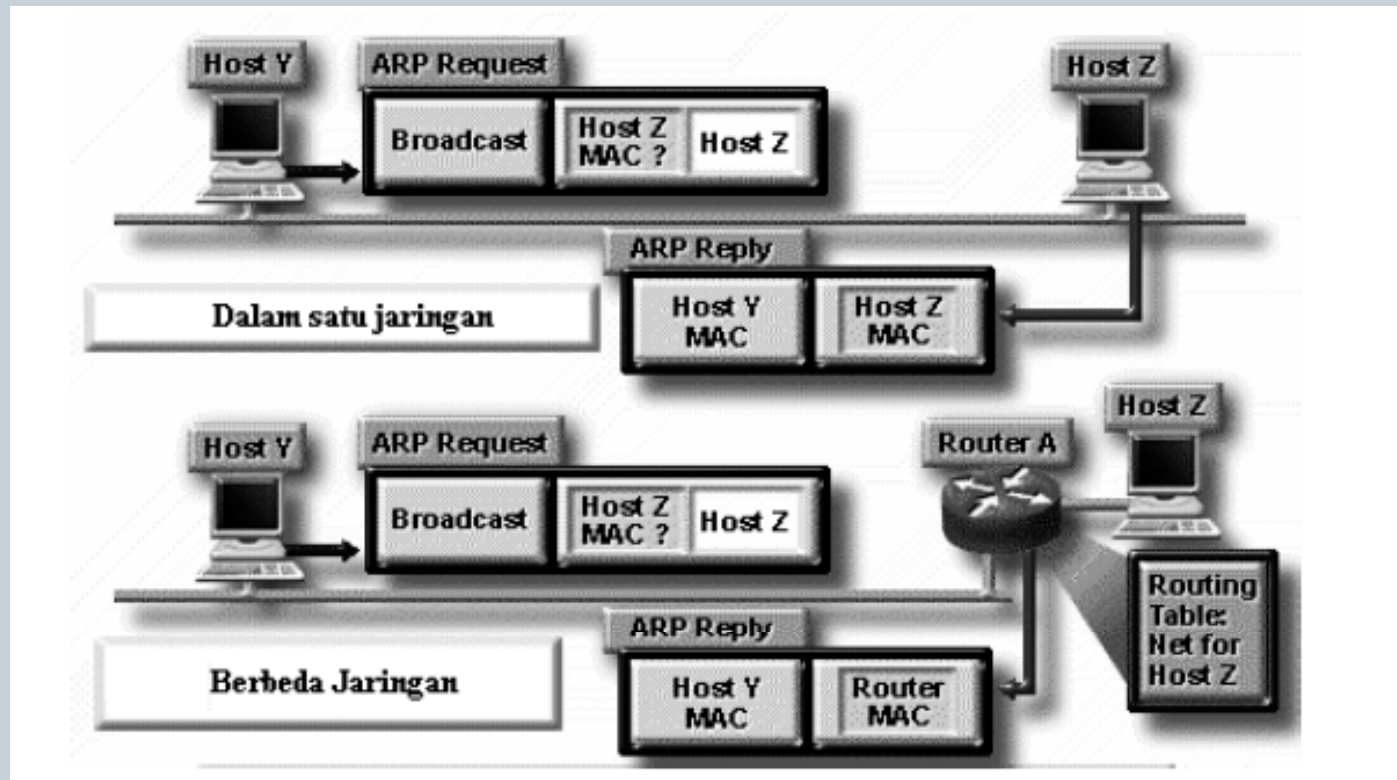
00-0C-04-17-91-CC

IP Destination Address IP Source Address Other IP fields and data

172.16.10.25 172.16.10.10

Cara Kerja protokol ARP

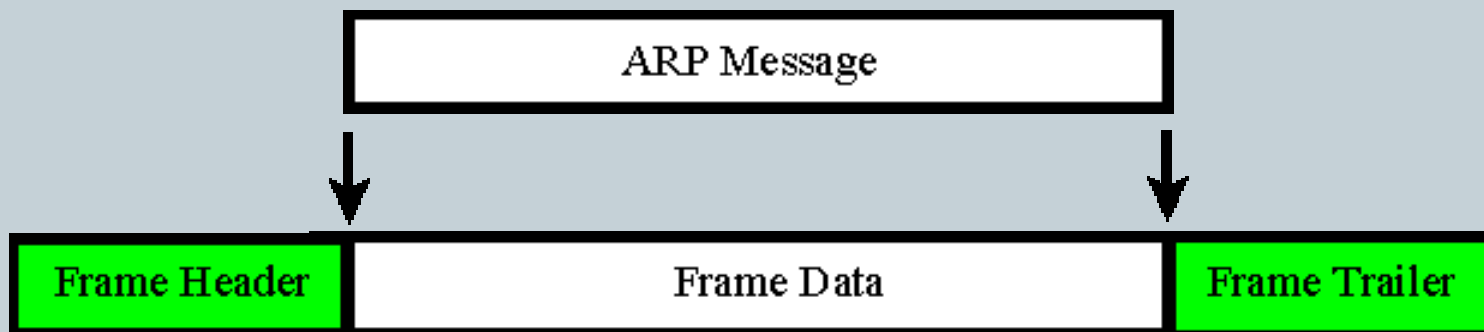
10



ARP Request

11

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

12

- **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

13

**NetBIOS
name**

resolve

**IP
address**

resolve

**MAC
address**

```
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

14

Nbtstat Output

Windows XP SP2

```
C:\>nbtstat -A 192.168.0.25
```

Local Area Connection:

Node IpAddress: [192.168.0.51] Scope Id: []

NetBIOS Remote Machine Name Table

Name	Type	Status
BEN-LAB25	<00> UNIQUE	Registered
STUDENTS	<00> GROUP	Registered
BEN-LAB25	<20> UNIQUE	Registered
STUDENTS	<1E> GROUP	Registered

MAC Address = 00-12-3F-C0-99-F9

Windows 2000/XP SP1

```
C:\>nbtstat -A 192.168.0.153
```

Local Area Connection:

Node IpAddress: [192.168.0.51] Scope Id: []

NetBIOS Remote Machine Name Table

Name	Type	Status
BEN-WS199700	<00> UNIQUE	Registered
LTU Domain	<00> GROUP	Registered
BEN-WS199700	<03> UNIQUE	Registered
BEN-WS199700	<20> UNIQUE	Registered
BEN-WS199700\$	<03> UNIQUE	Registered
LTU Domain	<1E> GROUP	Registered
BRUBBLE	<03> UNIQUE	Registered

MAC Address = 00-D4-23-0D-C8-55

Dynamic Host Configuration protocol

Pendahuluan

16

- 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...

17

- **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 ?

18

- Jaringan semakin besar dan semakin kompleks 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

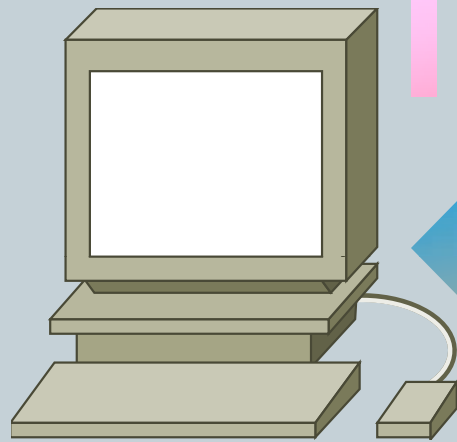
Sejarah DHCP Server

19

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

System Kerja RARP

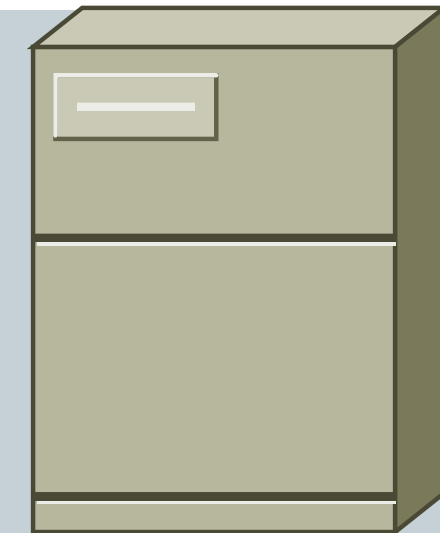
20



RARP Request

RARP Reply

Only IP Address



RARP server

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

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

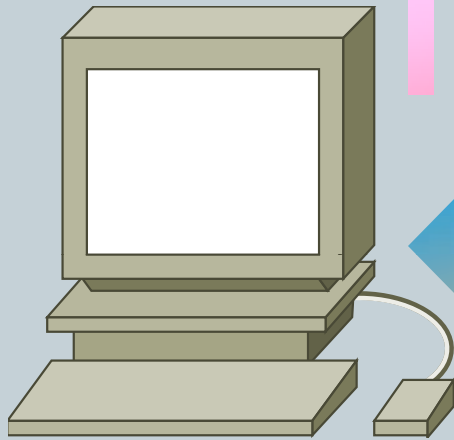
BOOTP

21

- 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

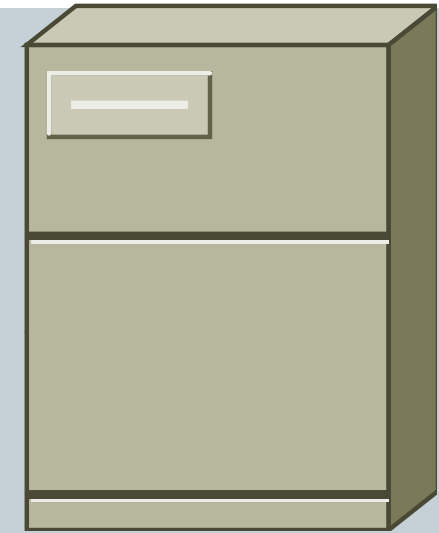
Sistem Kerja BOOTP

22



UDP Broadcast

UDP Broadcast



BOOTP server

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

IP Address
Gateway
IP server
Vendor-specific

MAC1 – IP1
MAC2 – IP2
MAC3 – IP3

Format Paket DHCP

23

- 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

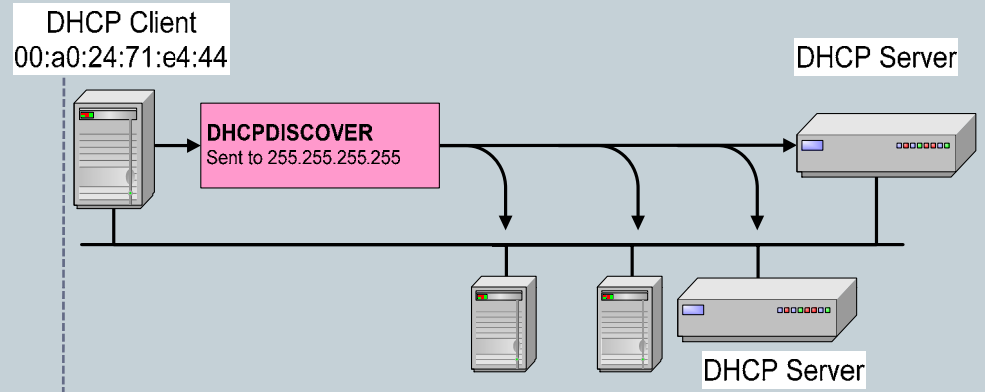
24

- Ketika DHCP client masuk/bergabung kedalam suatu jaringan, client tersebut 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 atau 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

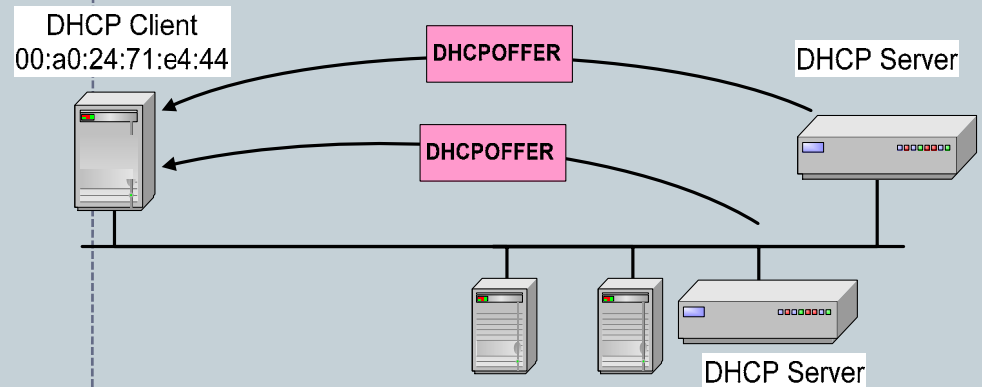
DHCP Operation

25

- DHCP DISCOVER



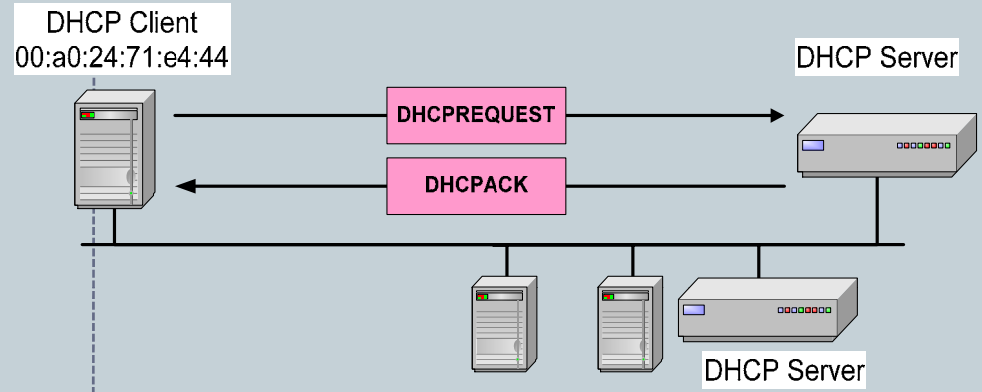
- DHCP OFFER



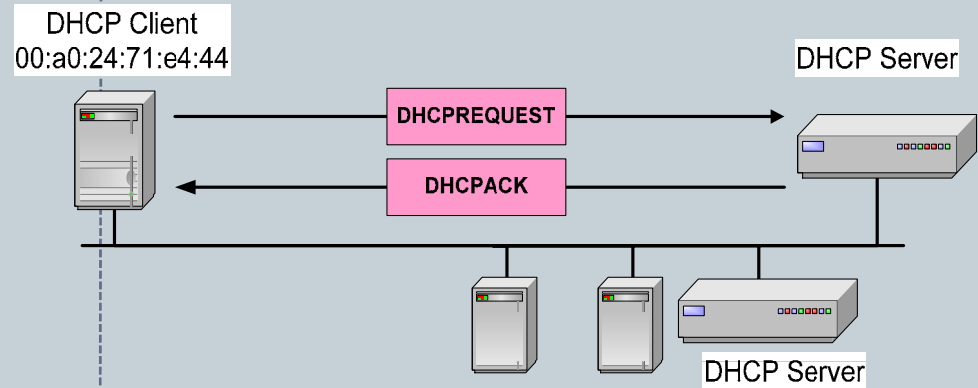
DHCP Operation

26

- DHCP REQUEST



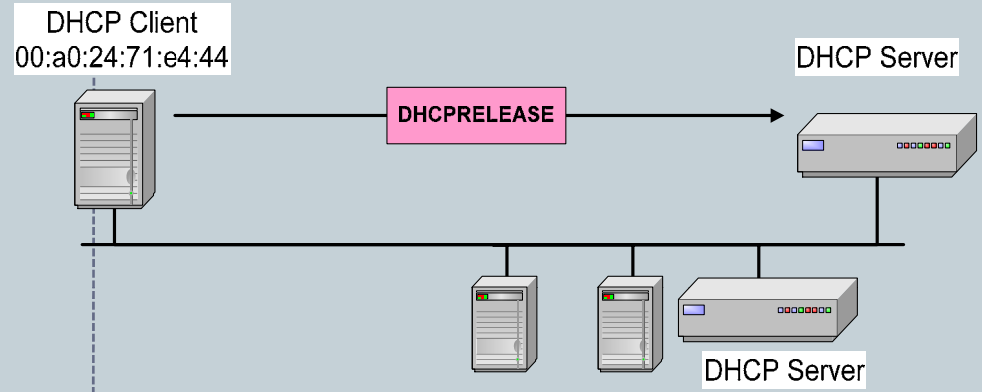
- DHCP ACK



DHCP Operation

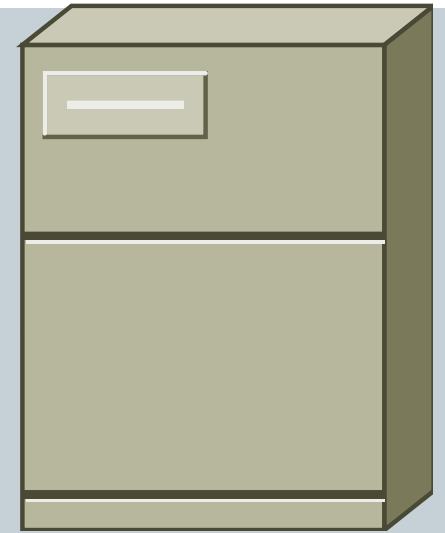
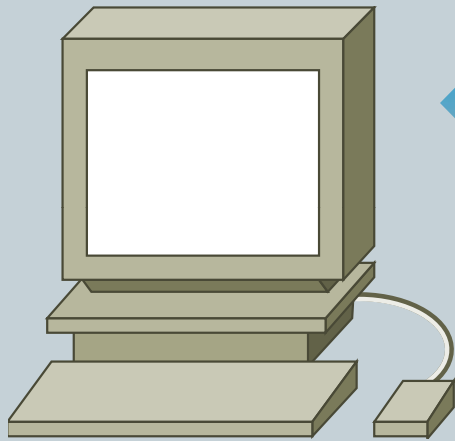
27

- DHCP RELEASE

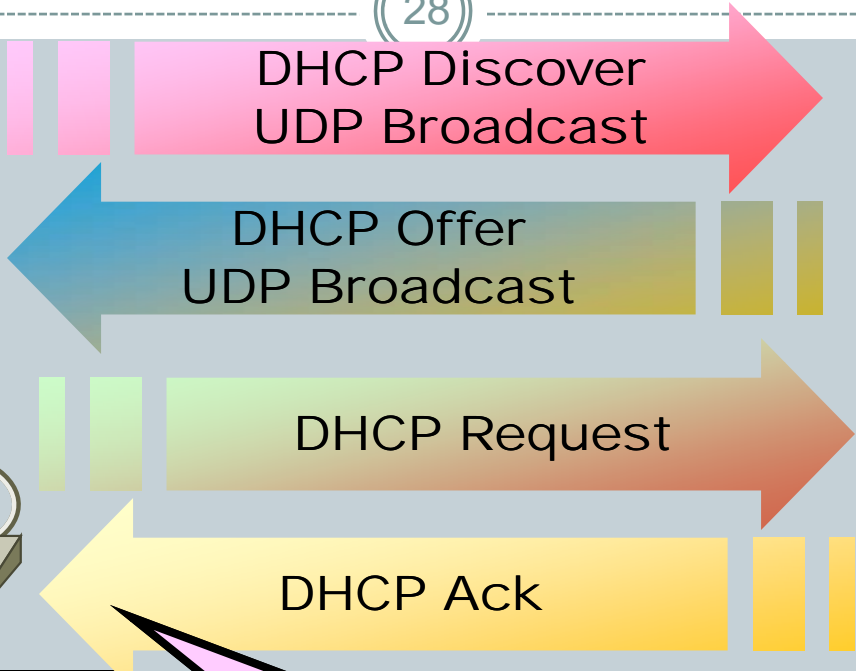


Sistem Kerja DHCP

28



DHCP server



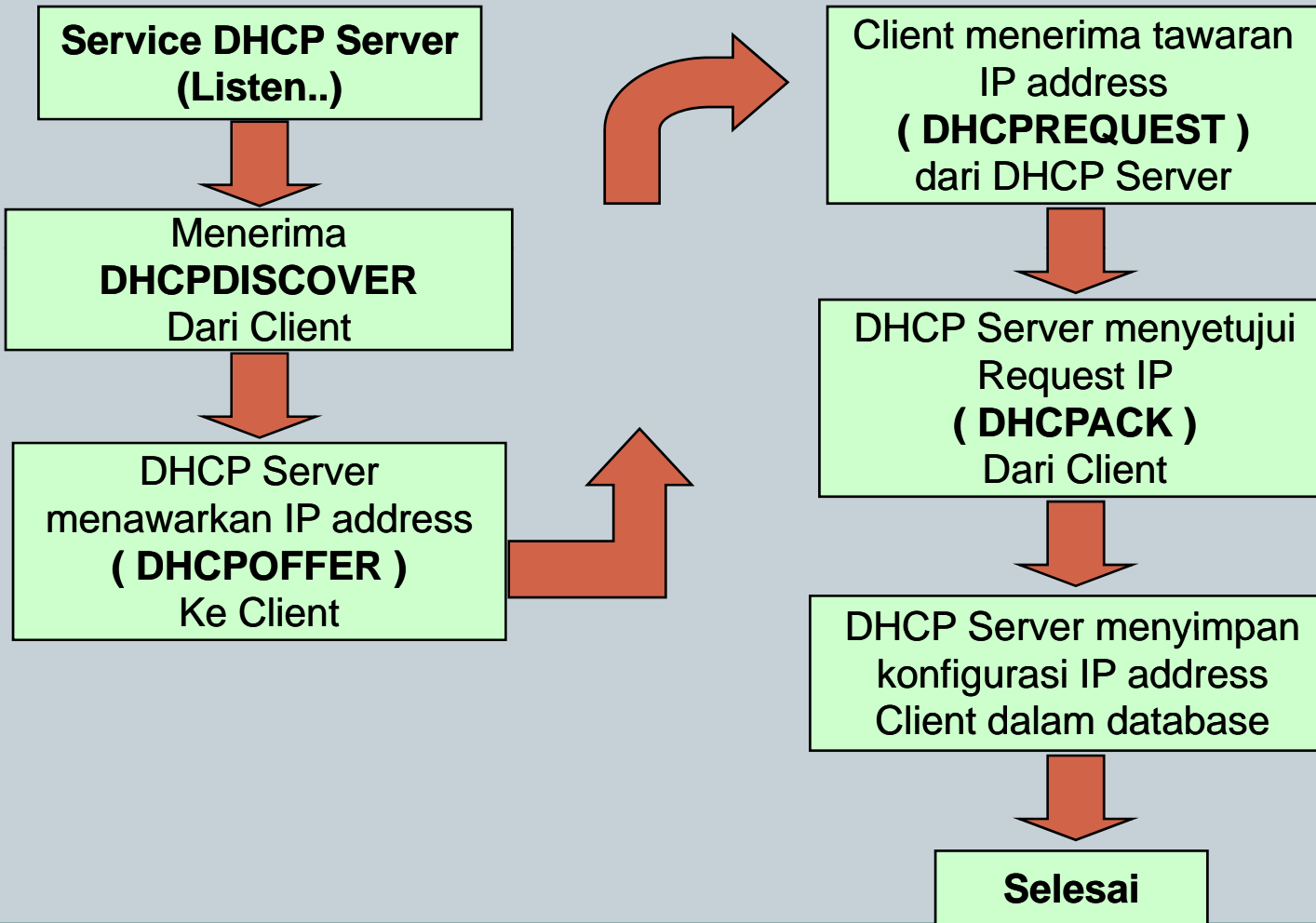
MAC: x:x:x:x:x:x
IP: ?

IP Address
Gateway
IP servers
Option lainnya...

IP1
IP2
IP3

Block Aliran Protocol DHCP

29



DHCP Message

30

- **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 Message 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

31

- **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 berturut-turut 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 dikodekan '8'.

Analisa Packet DHCP (DHCP Discover)

32

The screenshot displays the Wireshark interface with a packet capture of a DHCP Discover message. The packet list pane shows two packets: packet 11 (DHCP Discover) and packet 12 (DHCP Offer). Packet 11 is selected, and its details pane is expanded to show the DHCP Discover message structure.

No.	Time	Source	Destination	Protocol	Info
11	7.663055	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0xe86c3238
12	7.815308	192.168.0.222	255.255.255.255	DHCP	DHCP Offer - Transaction ID 0xe86c3238

Frame 11 (342 bytes on wire, 342 bytes captured)
Ethernet II, Src: 00:0c:29:6d:56:35, Dst: ff:ff:ff:ff:ff:ff
Internet Protocol, Src Addr: 0.0.0.0 (0.0.0.0), Dst Addr: 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: 0xe86c3238
 Seconds elapsed: 0
 Bootp flags: 0x8000 (Broadcast)
 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: 00:0c:29:6d:56:35 (192.168.0.10)
 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 = 192.168.0.93
 Option 12: Host Name = "v-xp-app"
 Option 60: Vendor class identifier = "MSFT 5.0"
 Option 55: Parameter Request List
 End option
 Padding

File: TA1 32 KB 00:02:33 | P: 294 D: 294 M: 0

Windows taskbar shows the Start button, active windows (Data (F:), cover.doc - Microsoft..., Bab V.doc - Microsoft..., Bab IV.doc - Microsoft..., TA1 - Ethereal), system tray (10:15, Jumat, 30/12/2005), and network status (Lagu (D:), eBooks, TA).

Analisa Packet DHCP (DHCP Offer)

33

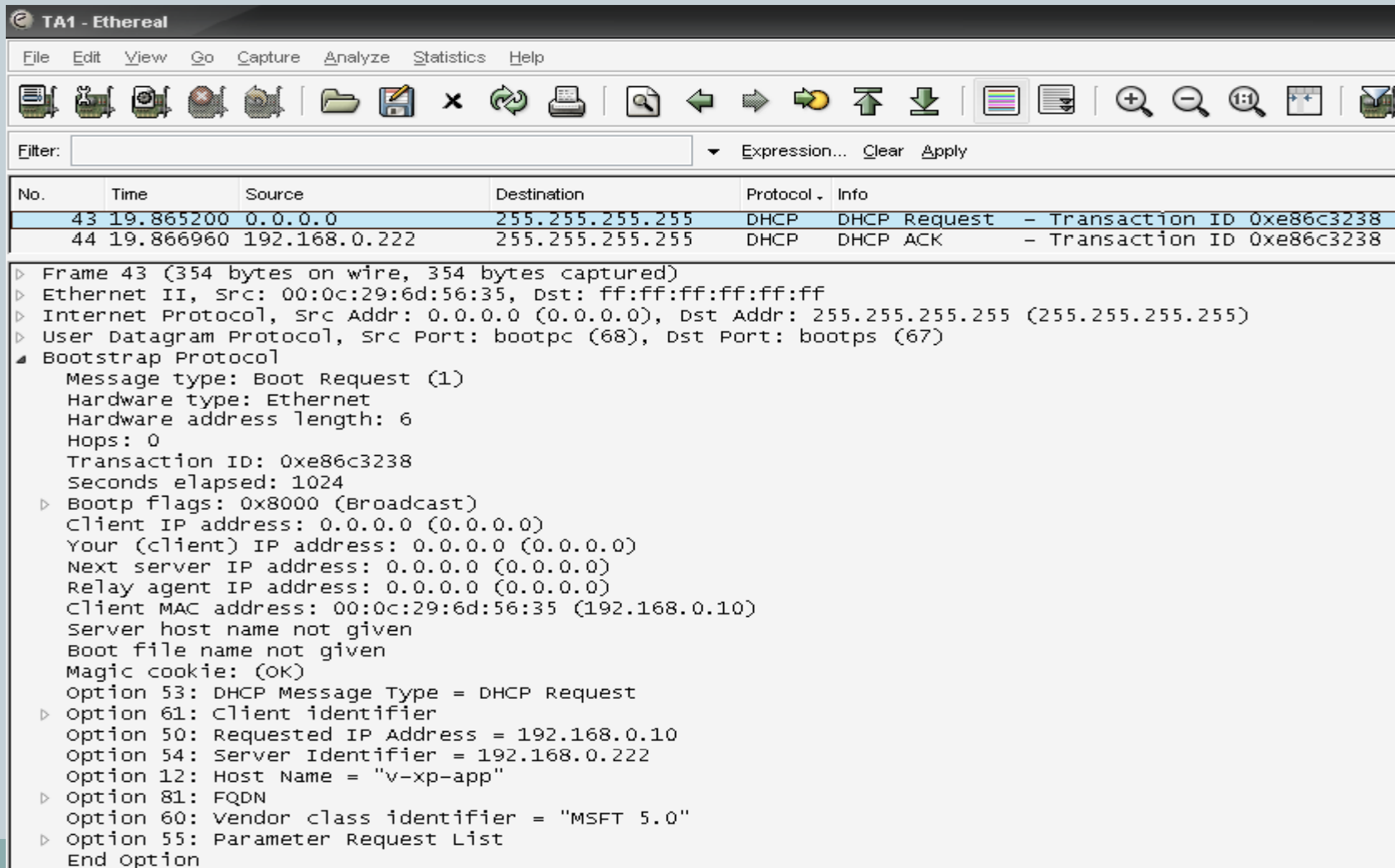
The screenshot displays the Wireshark interface with a packet capture of a DHCP Offer. The packet list pane shows two packets: packet 42 (DHCP Offer) and packet 43 (DHCP Request). Packet 42 is selected, and its details pane shows the following information:

- Frame 42 (590 bytes on wire, 590 bytes captured)
- Ethernet II, Src: 00:11:d8:20:06:bc, Dst: ff:ff:ff:ff:ff:ff
- Internet Protocol, Src Addr: 192.168.0.222 (192.168.0.222), Dst Addr: 255.255.255.255 (255.255.255.255)
- 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: 0xe86c3238
 - Seconds elapsed: 0
 - Bootp flags: 0x8000 (Broadcast)
 - Client IP address: 0.0.0.0 (0.0.0.0)
 - Your (client) IP address: 192.168.0.10 (192.168.0.10)
 - Next server IP address: 192.168.0.222 (192.168.0.222)
 - Relay agent IP address: 0.0.0.0 (0.0.0.0)
 - Client MAC address: 00:0c:29:6d:56:35 (192.168.0.10)
 - Server host name not given
 - Boot file name not given
 - Magic cookie: (OK)
 - option 54: Server Identifier = 192.168.0.222
 - option 53: DHCP Message Type = DHCP offer
 - option 51: IP Address Lease Time = 1 day, 12 hours, 10 minutes
 - option 6: Domain Name Server = 192.168.0.2
 - option 3: Router = 192.168.0.1
 - option 1: subnet Mask = 255.255.255.0
 - End option
 - Padding

The status bar at the bottom indicates the file is TA1 (32 KB, 00:02:33) and the packet is 294 D, 294 M, 0. The taskbar shows the Start button, several open documents, and the system clock at 10:30 on 30/12/2005.

Analisa Packet DHCP (DHCP Request)

34



The screenshot displays the Wireshark interface for a packet capture named 'TA1 - Ethereal'. The packet list pane shows two packets:

No.	Time	Source	Destination	Protocol	Info
43	19.865200	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0xe86c3238
44	19.866960	192.168.0.222	255.255.255.255	DHCP	DHCP ACK - Transaction ID 0xe86c3238

The packet details pane for packet 43 shows the following structure:

- Frame 43 (354 bytes on wire, 354 bytes captured)
- Ethernet II, Src: 00:0c:29:6d:56:35, Dst: ff:ff:ff:ff:ff:ff
- Internet Protocol, Src Addr: 0.0.0.0 (0.0.0.0), Dst Addr: 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: 0xe86c3238
 - Seconds elapsed: 1024
 - Bootp flags: 0x8000 (Broadcast)
 - 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: 00:0c:29:6d:56:35 (192.168.0.10)
 - 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 = 192.168.0.10
 - Option 54: Server Identifier = 192.168.0.222
 - Option 12: Host Name = "v-xp-app"
 - Option 81: FQDN
 - Option 60: Vendor class identifier = "MSFT 5.0"
 - Option 55: Parameter Request List
 - End option

Analisa Packet DHCP (DHCP Ack)

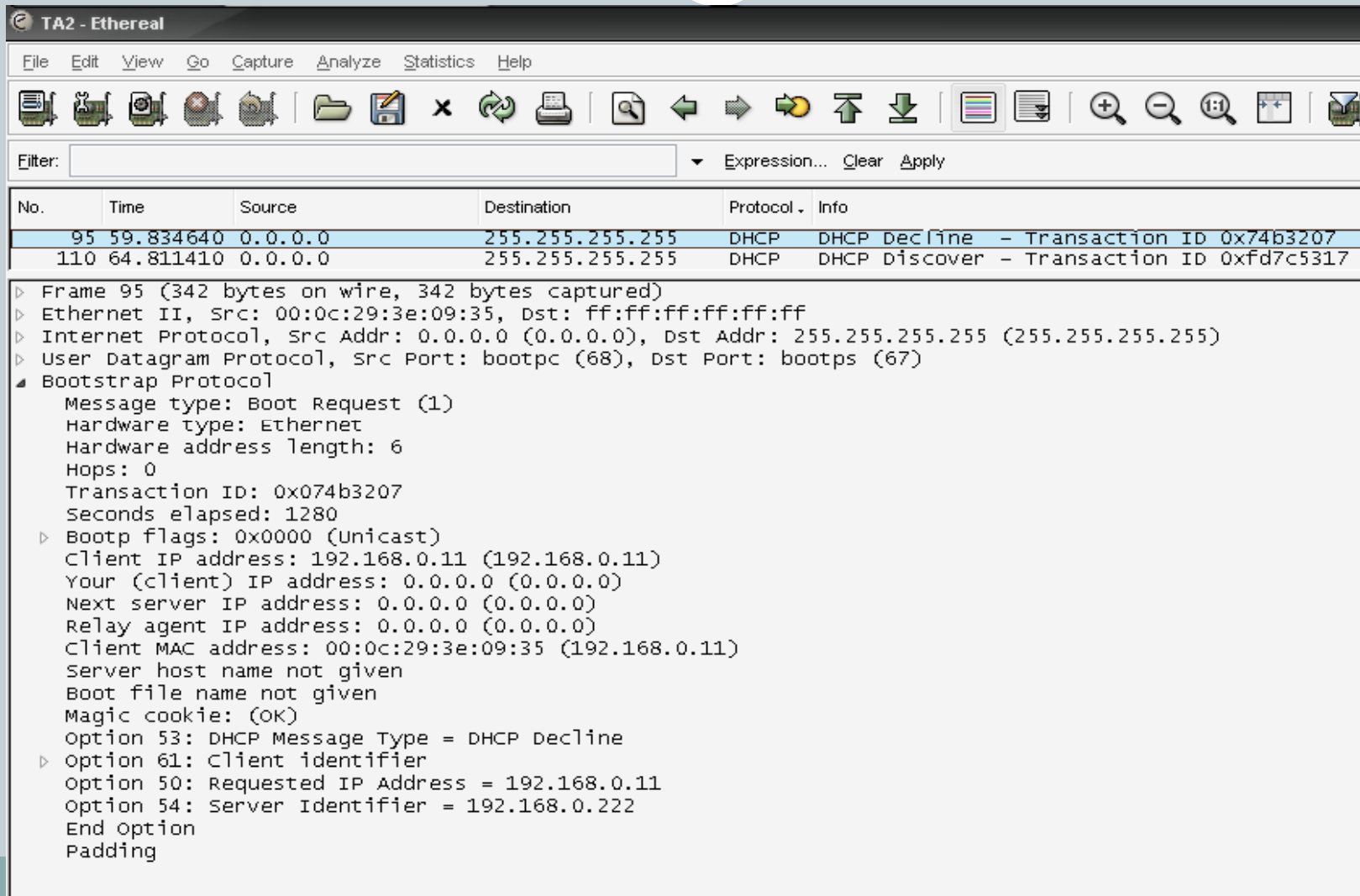
35

The screenshot shows the Wireshark interface for a capture named 'TA1 - Ethereal'. The packet list pane shows two packets: packet 43 is a DHCP Request and packet 44 is a DHCP ACK. Packet 44 is selected, and its details pane is expanded to show the following information:

- Frame 44 (590 bytes on wire, 590 bytes captured)
- Ethernet II, Src: 00:11:d8:20:06:bc, Dst: ff:ff:ff:ff:ff:ff
- Internet Protocol, Src Addr: 192.168.0.222 (192.168.0.222), Dst Addr: 255.255.255.255 (255.255.255.255)
- User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
- Bootstrap Protocol
 - Message type: Boot Reply (2)
 - Hardware type: Ethernet
 - Hardware address length: 0
 - Hops: 0
 - Transaction ID: 0xe86c3238
 - Seconds elapsed: 0
 - Bootp flags: 0x8000 (Broadcast)
 - Client IP address: 0.0.0.0 (0.0.0.0)
 - Your (client) IP address: 192.168.0.10 (192.168.0.10)
 - 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: 00:0c:29:6d:56:35 (192.168.0.10)
 - Server host name not given
 - Boot file name not given
 - Magic cookie: (OK)
 - Option 54: Server Identifier = 192.168.0.222
 - Option 53: DHCP Message Type = DHCP ACK
 - Option 51: IP Address Lease Time = 1 day, 12 hours, 10 minutes
 - Option 6: Domain Name Server = 192.168.0.2
 - Option 3: Router = 192.168.0.1
 - Option 1: Subnet Mask = 255.255.255.0
 - End Option
 - Padding

Analisa Packet DHCP (DHCP Decline)

36



The screenshot shows the Wireshark interface with the following details:

- Filter:** Expression... Clear Apply
- Packet List:**

No.	Time	Source	Destination	Protocol	Info
95	59.834640	0.0.0.0	255.255.255.255	DHCP	DHCP Decline - Transaction ID 0x74b3207
110	64.811410	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0xfd7c5317
- Packet 95 Details:**
 - Frame 95 (342 bytes on wire, 342 bytes captured)
 - Ethernet II, Src: 00:0c:29:3e:09:35, Dst: ff:ff:ff:ff:ff:ff
 - Internet Protocol, Src Addr: 0.0.0.0 (0.0.0.0), Dst Addr: 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: 0x074b3207
 - Seconds elapsed: 1280
 - Bootp flags: 0x0000 (Unicast)
 - Client IP address: 192.168.0.11 (192.168.0.11)
 - 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: 00:0c:29:3e:09:35 (192.168.0.11)
 - Server host name not given
 - Boot file name not given
 - Magic cookie: (OK)
 - Option 53: DHCP Message Type = DHCP Decline
 - Option 61: Client identifier
 - Option 50: Requested IP Address = 192.168.0.11
 - Option 54: Server Identifier = 192.168.0.222
 - End Option
 - Padding