JARINGAN KOMPUTER – TUGAS PENDAHULUAN MODUL 11
DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)

Nama : Muhammad Hamzah Haifan Ma'ruf

NIM : 2311102091

Kelas : S1IF-11-07

Kode Dosen : AIZ

JAWABAN MODUL

A. Teori

1. Hubungan Layer OSI Model dan TCP/IP Model

   Model OSI dan TCP/IP merupakan dua kerangka kerja yang digunakan untuk memahami cara kerja komunikasi jaringan. OSI Model terdiri dari tujuh lapisan: Application, Presentation, Session, Transport, Network, Data Link, dan Physical. Sementara itu, TCP/IP Model hanya memiliki empat lapisan: Application, Transport, Internet, dan Network Access. Hubungan antara keduanya adalah sebagai berikut: Application, Presentation, dan Session Layer pada OSI digabung menjadi Application Layer dalam TCP/IP; Transport Layer tetap sama pada kedua model; Network Layer pada OSI setara dengan Internet Layer pada TCP/IP; serta Data Link dan Physical Layer digabung menjadi Network Access Layer dalam TCP/IP. Beberapa protokol jaringan umum berada pada layer-layer tertentu dalam kedua model tersebut. Protokol seperti HTTP, FTP, SMTP, DNS, dan DHCP berada di Application Layer baik dalam OSI maupun TCP/IP. TCP dan UDP berada di Transport Layer untuk kedua model. Protokol IP berada di Network Layer pada OSI dan Internet Layer dalam TCP/IP.

2. IPv4 Proses Alokasi IP oleh DHCP (Mekanisme DORA)

   Proses alokasi alamat IP oleh DHCP menggunakan mekanisme yang disebut DORA, yang merupakan singkatan dari Discover, Offer, Request, dan Acknowledge. Pertama, klien yang baru menyambung ke jaringan akan mengirimkan pesan DHCP Discover sebagai broadcast untuk mencari server DHCP yang tersedia. Kedua, server DHCP yang menerima

permintaan tersebut akan mengirimkan DHCP Offer yang berisi alamat IP yang tersedia serta informasi konfigurasi lainnya. Ketiga, klien memilih satu tawaran dan mengirimkan DHCP Request untuk mengonfirmasi pilihannya kepada server. Keempat, server akan membalas dengan DHCP Acknowledge sebagai tanda persetujuan akhir bahwa alamat IP tersebut telah dialokasikan untuk klien. Tujuan dari tiap tahap ini adalah memastikan klien mendapatkan alamat IP yang unik dan sah digunakan di dalam jaringan.

3. Peran Subnetting dalam Alokasi IP oleh DHCP

   Subnetting memainkan peran penting dalam pengelolaan dan alokasi alamat IP oleh server DHCP karena memungkinkan jaringan besar dibagi menjadi beberapa bagian kecil atau subnet. Dengan cara ini, administrator jaringan dapat membagi alokasi IP sesuai kebutuhan masing-masing segmen jaringan. Ketika sebuah jaringan dibagi menjadi beberapa subnet, DHCP dapat dikonfigurasi untuk menyediakan alamat IP yang sesuai dengan masing-masing subnet, sehingga setiap klien dalam satu subnet akan menerima IP dari rentang yang sesuai. Dalam jaringan dengan banyak segmen, DHCP juga dapat menggunakan DHCP relay untuk menjangkau server DHCP di luar subnet lokal. Dengan begitu, subnetting tidak hanya mempermudah manajemen IP tetapi juga mengurangi lalu lintas broadcast dan meningkatkan efisiensi jaringan.

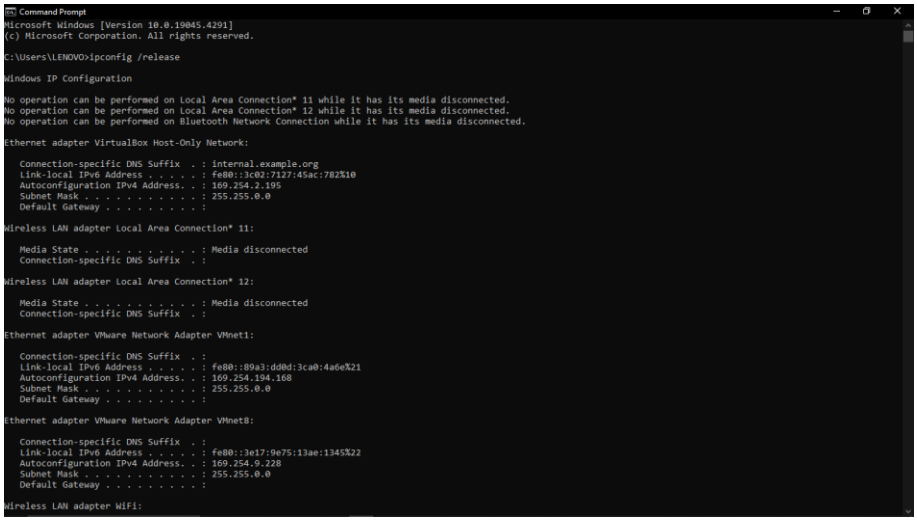
4. Penjelasan mod11theory dan Konfigurasi DHCP

   File atau link bernama mod11theory.gif kemungkinan besar merupakan gambar topologi jaringan sederhana yang menunjukkan bagaimana DHCP digunakan untuk mengelola alokasi alamat IP secara otomatis. Misalnya, perangkat seperti PC0 hingga PC4 akan diatur agar menerima IP secara otomatis dari server DHCP tanpa perlu konfigurasi manual. Dalam skenario ini, DHCP dapat dikonfigurasi pada sebuah router agar bertindak sebagai server DHCP. Konfigurasi tersebut melibatkan pembuatan DHCP pool yang berisi rentang alamat IP, pengaturan default gateway, DNS server, dan pengecualian alamat-alamat IP tertentu yang tidak boleh dibagikan. Secara umum, router dapat berfungsi sebagai DHCP server dengan konfigurasi yang tepat, sedangkan switch biasa (layer-2) tidak dapat menjadi DHCP server, kecuali jika menggunakan switch layer-3 yang mendukung fungsi tersebut. Dengan konfigurasi ini, DHCP sangat membantu dalam mengelola IP address secara efisien dan otomatis di jaringan yang memiliki banyak perangkat klien.

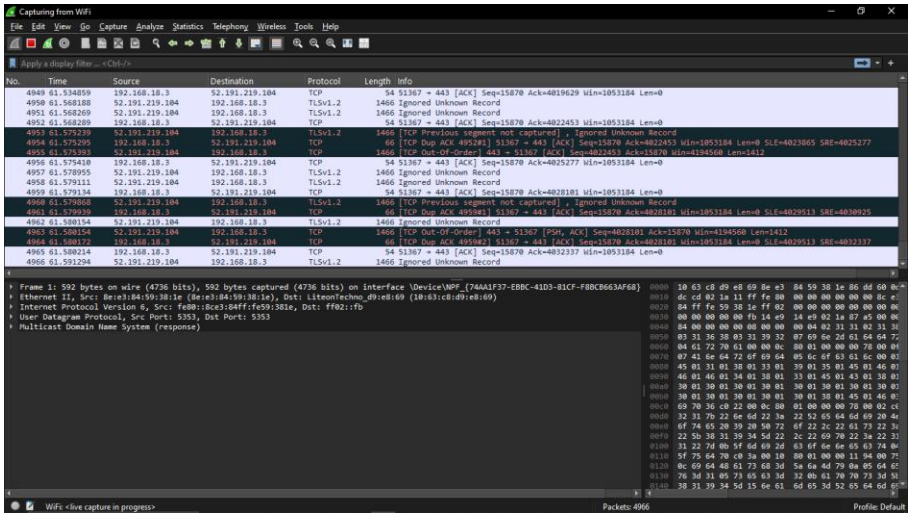
B. Gathering a Packet Trace

   1. Di jendela/shell terminal, masukkan command berikut:
      ipconfig / release

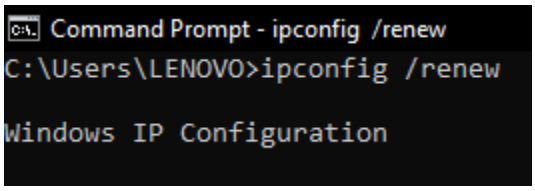
(Note: Command ini akan menyebabkan PC anda memberikan alamat IP nya)



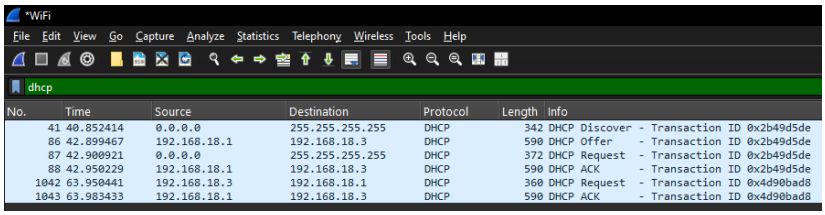
2. Mulai Wireshark



3. Di jendela/shell terminal, masukkan command berikut:
ipconfig / renew



4. Pastikan paket DHCP tertangkap, hetikan capture paket Wireshark.



C. IPv4 Advance part 2 (IPv4 Subnetting)

1. Lakukan alokasi IP menggunakan metode VLSM, FLSM, dan CIDR

   VLSM (Variable Length Subnet Masking). VLSM memungkinkan kita untuk mengalokasikan subnet dengan ukuran yang berbeda-beda sesuai dengan kebutuhan host masing-masing. Dalam hal ini, kita memiliki kebutuhan subnet dengan jumlah host yang berbeda, yaitu:

   - Net_A: 120 host
   - Net_B: 50 host
   - Net_C: 16 host
   - Antar Router: 2 host

   Langkah pertama adalah menentukan jumlah bit yang dibutuhkan untuk setiap subnet. Kita gunakan rumus untuk menghitung jumlah bit untuk subnet yang dibutuhkan, yaitu:

   Jumlah host yang dibutuhkan=2n−2
   Di mana n adalah jumlah bit untuk host.
   Perhitungan untuk setiap subnet:

   - Net_A (120 host):
     2^7 - 2 = 128 - 2 = 126 host
     Jadi, kita membutuhkan subnet dengan ukuran 128 host (atau /25).

- Net_B (50 host):
  2^6 - 2 = 64 - 2 = 62 host
  Jadi, kita membutuhkan subnet dengan ukuran 64 host (atau /26).
- Net_C (16 host):
  2^5 - 2 = 32 - 2 = 30 host
  Jadi, kita membutuhkan subnet dengan ukuran 32 host (atau /27).
- Antar Router (2 host):
  2^2 - 2 = 4 - 2 = 2 host
  Jadi, kita membutuhkan subnet dengan ukuran 4 host (atau /30).

FLSM (Fixed Length Subnet Masking). FLSM menggunakan subnet mask yang sama untuk setiap subnet. Dalam hal ini, kita akan mencari subnet dengan ukuran yang cukup untuk menampung subnet yang terbesar (Net_A dengan 120 host). Dari perhitungan sebelumnya, Net_A membutuhkan /25, yang artinya setiap subnet akan menggunakan /25 untuk menampung 128 host.

CIDR (Classless Inter-Domain Routing). CIDR adalah cara untuk menentukan subnet tanpa memperhatikan batasan kelas jaringan yang kaku. CIDR menggunakan format "IP/Prefix", seperti yang sudah dilakukan di atas. Kita sudah mengalokasikan subnet berdasarkan CIDR, yang sesuai dengan /25, /26, /27, dan /30.

2. Berdasarkan hasil VLSM! Tentukan range IP yang dialokasikan untuk DHCP Server! Sisihkan beberapa IP untuk perangkat statis (misalnya gateway, server)! Tampilkan jumlah IP yang tersedia untuk distribusi DHCP

   Untuk VLSM, mari kita alokasikan rentang IP untuk masing-masing subnet sesuai dengan kebutuhan, sambil menyisihkan beberapa IP untuk perangkat statis (misalnya gateway, server).

   - Net_A (120 host):
     - Subnet: 10.120.30.0/25
     - Rentang IP: 10.120.30.1 - 10.120.30.126
     - IP yang digunakan untuk perangkat statis: 10.120.30.1 (Gateway, Server, dsb.)
     - Rentang DHCP: 10.120.30.2 - 10.120.30.126 (Total 125 IP yang tersedia)

   - Net_B (50 host):
     - Subnet: 10.120.30.128/26

  - Rentang IP: 10.120.30.129 - 10.120.30.190
  - IP yang digunakan untuk perangkat statis: 10.120.30.129 (Gateway, Server, dsb.)
  - Rentang DHCP: 10.120.30.130 - 10.120.30.190 (Total 61 IP yang tersedia)

- Net_C (16 host):
  - Subnet: 10.120.30.192/27
  - Rentang IP: 10.120.30.193 - 10.120.30.222
  - IP yang digunakan untuk perangkat statis: 10.120.30.193 (Gateway, Server, dsb.)
  - Rentang DHCP: 10.120.30.194 - 10.120.30.222 (Total 29 IP yang tersedia)

- Antar Router (2 host):
  - Subnet: 10.120.30.224/30
  - Rentang IP: 10.120.30.225 - 10.120.30.226
  - IP yang digunakan untuk perangkat statis: 10.120.30.225 (Gateway Antar Router)
  - Rentang DHCP: Tidak diperlukan untuk antar router karena hanya 2 IP yang digunakan.

3. Jelaskan bagaimana DHCP bekerja dalam topologi ini!

   DHCP (Dynamic Host Configuration Protocol) adalah protokol yang memungkinkan perangkat di jaringan untuk mendapatkan pengaturan IP secara otomatis dari server DHCP, tanpa memerlukan konfigurasi manual. Dalam topologi ini:

   - Server DHCP akan diberikan rentang IP dinamis untuk setiap subnet (seperti yang telah dihitung di atas).
   - Ketika perangkat (misalnya komputer, printer, atau perangkat lain) terhubung ke jaringan, perangkat tersebut akan mengirimkan permintaan DHCP ke server DHCP.
   - Server DHCP akan merespons dengan memberikan alamat IP yang sesuai dari rentang IP yang dialokasikan untuk subnet tersebut. Server DHCP juga akan memberikan informasi tambahan seperti gateway dan DNS.
   - Gateway di setiap subnet akan digunakan untuk menghubungkan perangkat dalam subnet tersebut ke jaringan luar (misalnya internet).

Pada setiap subnet, ada rentang IP yang disisihkan untuk perangkat statis, yang umumnya meliputi gateway, server, dan perangkat lainnya yang memerlukan IP tetap. Sedangkan IP lainnya akan diberikan secara dinamis kepada perangkat yang membutuhkan koneksi jaringan.

D. Socket Programming with DHCP

1. Mekanisme Alokasi IP dan Dampaknya jika Klien Melebihi Kapasitas

   Ketika lima klien mencoba mendapatkan alamat IP secara bersamaan dari server DHCP, dan hanya tersedia empat alamat IP dalam pool, maka klien kelima tidak akan mendapatkan alamat IP. Hal ini terjadi karena server DHCP hanya dapat mendistribusikan IP sesuai dengan jumlah yang tersedia. Dalam kode dhcp_server.py, terdapat mekanisme lease time yang mengatur lamanya sebuah IP dapat digunakan oleh klien. Setelah lease time habis, alamat IP yang sebelumnya diberikan akan kembali masuk ke pool dan bisa digunakan kembali oleh klien lain. Dengan demikian, kode ini memastikan bahwa alamat IP yang telah digunakan dapat didaur ulang secara efisien setelah masa berlakunya berakhir, mencegah pemborosan sumber daya IP dalam jaringan.

2. Pentingnya Lease Time dalam Efisiensi Jaringan DHCP

   Klien perlu meminta alamat IP baru setelah lease time habis agar IP yang digunakan tidak terus menerus dikunci oleh satu perangkat, terutama jika perangkat tersebut sudah tidak aktif lagi di jaringan. Mekanisme ini penting karena memberikan efisiensi dalam pemanfaatan alamat IP, terutama di jaringan yang jumlah IP-nya terbatas. Lease time memungkinkan sistem untuk melakukan rotasi IP dan memberikan IP kepada klien baru yang membutuhkannya. Jika lease time diatur terlalu pendek, misalnya hanya 10 detik, maka klien akan sering melakukan permintaan pembaruan IP (renewal). Hal ini dapat meningkatkan beban komunikasi antara klien dan server DHCP serta menurunkan performa jaringan secara keseluruhan karena meningkatnya lalu lintas DHCP yang tidak perlu.

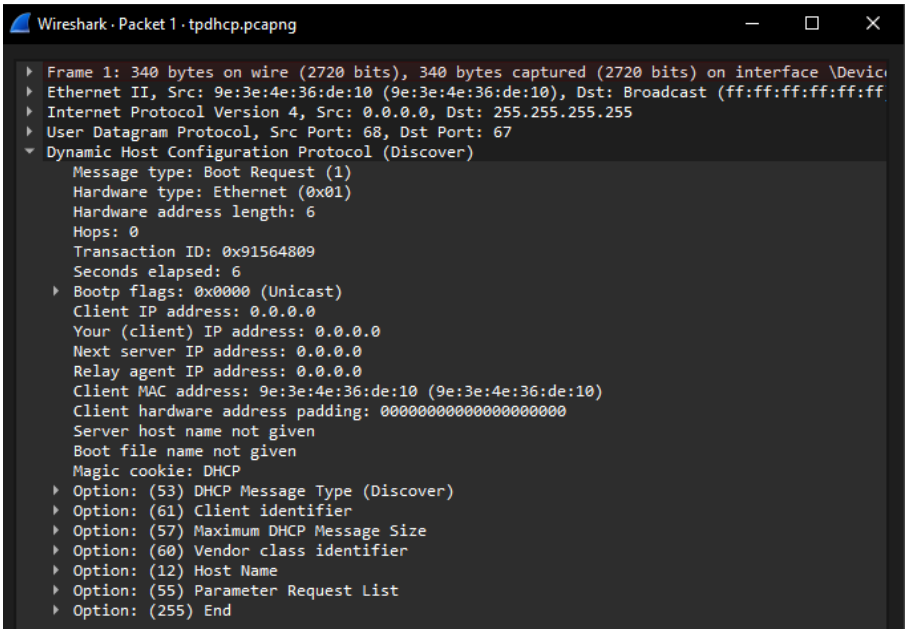
3. Analisis Kegagalan DHCP pada Klien Pertama dan Langkah Penyelesaiannya

   Klien pertama dengan MAC address AA:AA:AA:AA:AA:AA tidak menerima DHCP Offer dari server, meskipun sudah mengirimkan DHCP Discover. Hal ini bisa terjadi karena beberapa kemungkinan, di antaranya jumlah IP pada server telah habis sehingga tidak ada lagi yang bisa diberikan kepada klien tersebut.

Kemungkinan lainnya adalah MAC address tersebut telah tercatat pada server sebagai klien aktif dan belum melewati masa lease-nya, sehingga server menolak untuk mengalokasikan kembali alamat IP. Selain itu, jika banyak klien mengirim permintaan secara bersamaan, bisa terjadi kondisi balapan (race condition) atau blocking I/O di mana permintaan dari klien pertama tidak sempat diproses oleh server tepat waktu. Untuk menyelesaikan masalah ini, langkah debugging yang dapat dilakukan adalah memeriksa log di dhcp_server.py, memastikan bahwa permintaan dari klien pertama benar-benar diterima, menambahkan pesan log untuk semua permintaan dan alokasi IP, serta menjalankan klien satu per satu agar dapat melihat proses kerja server secara bertahap. Dengan membandingkan output antara Terminal 2 dan Terminal 3, kita dapat melihat bahwa klien lain berhasil mendapatkan respons DHCP secara lengkap, sementara klien pertama tidak. Perbedaan ini menunjukkan bahwa analisis terhadap urutan request dan ketersediaan IP sangat penting untuk memahami penyebab kegagalan distribusi IP.

E. Wireshark DHCP

1. DHCP Discover



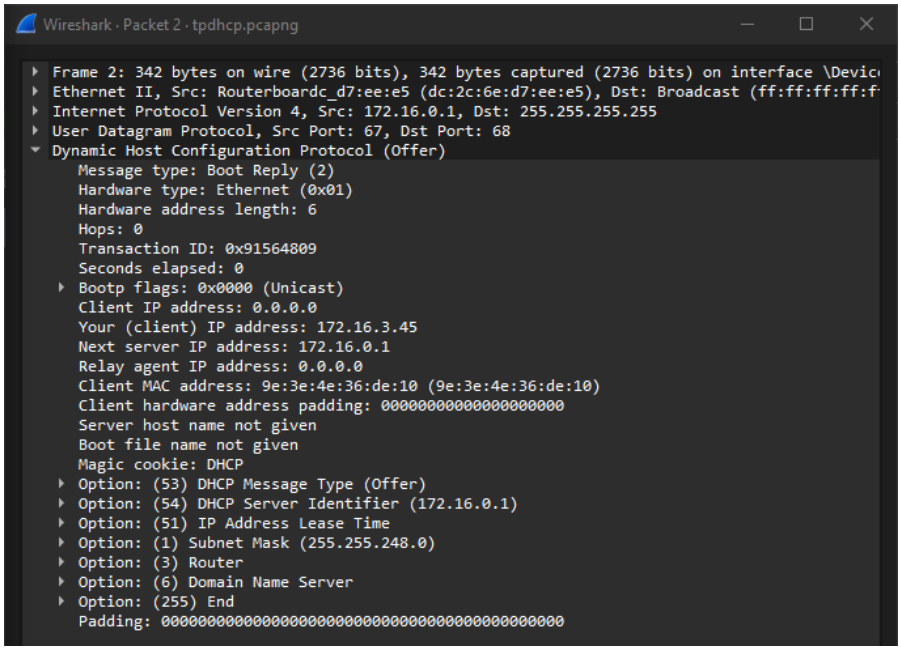
DHCP Discover terjadi di Packet No. 1 pada waktu 0.000000 sec.
Dapat dikenali dari:

- Message type: Boot Request

- DHCP Message Type: DHCP Discover (1)

2. Transaction ID
   Transaction ID: 0x91564809. Semua paket dalam satu siklus DORA menggunakan Transaction ID yang sama, ini digunakan untuk mencocokkan bahwa pesan itu bagian dari satu transaksi DHCP.

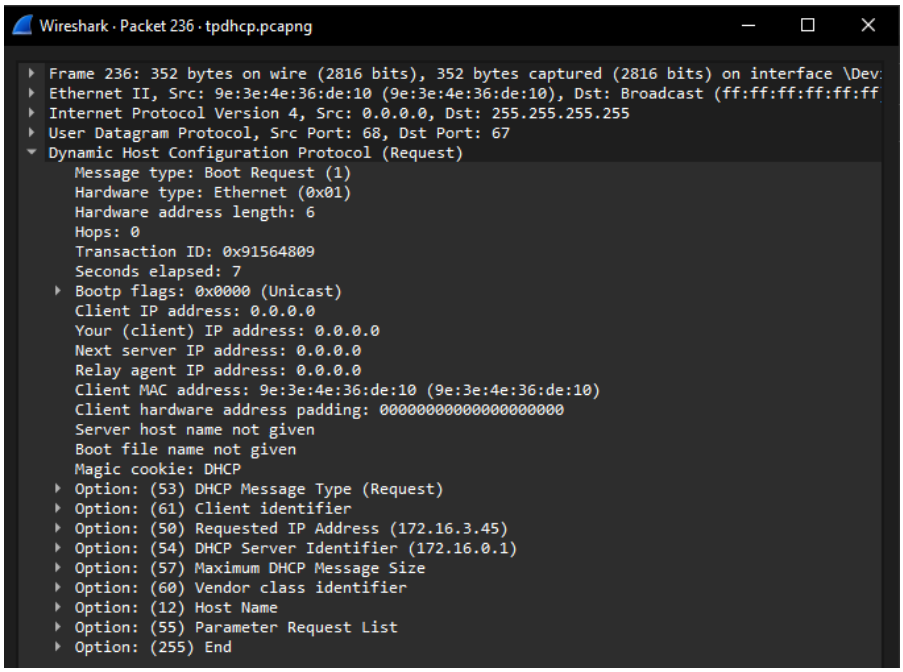
3. DHCP Offer



   DHCP Offer dikirim di Packet No. 2
   Pengirim: DHCP Server 172.16.0.1
   IP yang ditawarkan: Your (client) IP address: 172.16.3.45

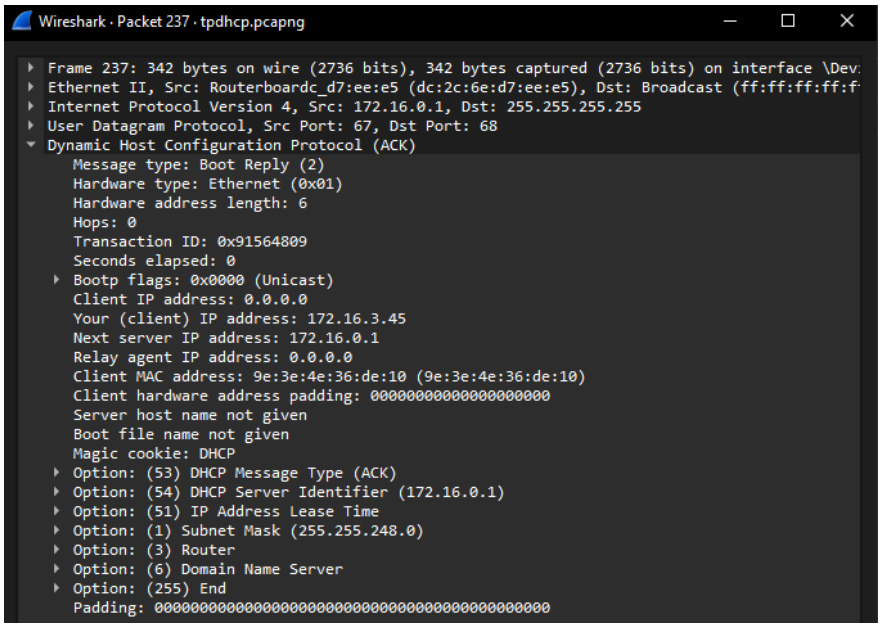
4. DHCP Server Identifier
   DHCP Server Identifier (172.16.0.1). Ini menunjukkan IP dari server yang memberikan Offer, sehingga klien tahu harus membalas ke server tersebut dalam DHCP Request.

5. DHCP Request



DHCP Request terjadi di Packet No. 236
Tujuannya: Memberi tahu server bahwa klien menerima tawaran IP. Klien menunjukkan penerimaan dengan mencantumkan opsi Requested IP Address dan Server Identifier di paket.

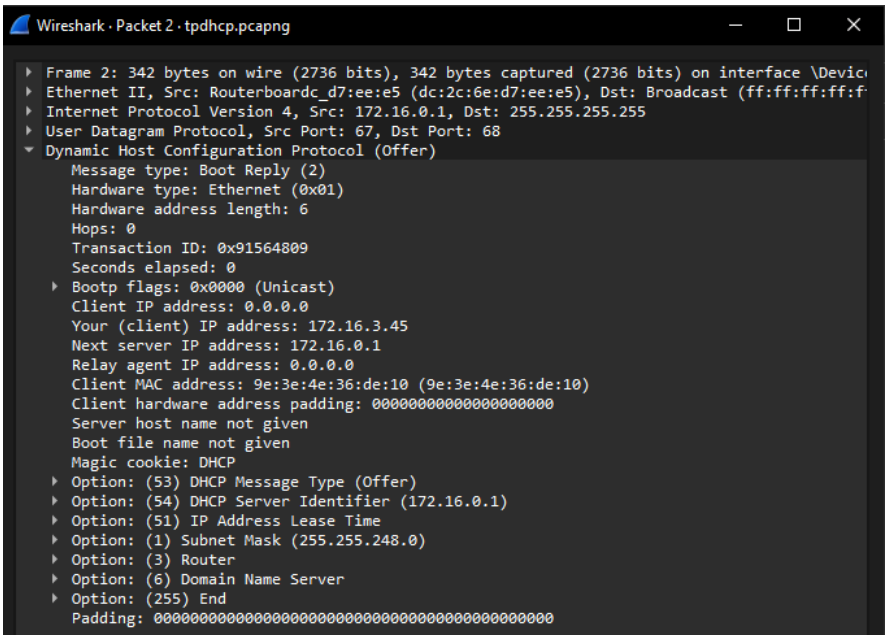
6. DHCP ACK



DHCP ACK diterima di Packet No. 237
Informasi penting:

- Your (client) IP address: 172.16.3.45
- IP Address Lease Time: 1 day (86400)
- Subnet Mask: 255.255.248.0

7. Parameter Jaringan dalam DHCP Offer/ACK



Subnet Mask: 255.255.248.0
Router (Default Gateway): 172.16.0.1
Domain Name Server: 202.51.96.7
Domain Name Server: 202.51.102.118

8. Urutan DHCP DORA Lengkap

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	340	DHCP Discover - Transaction ID 0x91564809
2	0.000000	172.16.0.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x91564809
236	1.222170	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0x91564809
237	1.222170	172.16.0.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x91564809

Urutan DORA:

- Discover – Paket No. 1
- Offer – Paket No. 2
- Request – Paket No. 236
- ACK – Paket No. 237

Penjelasan:
Proses DORA memastikan bahwa

- Klien menemukan DHCP server (Discover)
- Server menawarkan alamat IP (Offer)
- Klien secara eksplisit memilih satu server dan alamat (Request)
- Server mengonfirmasi dan memberikan IP secara resmi (ACK)