

Fungsi *Address Resolution Protocol* dalam Ethernet

(*Address Resolution Protocol Functions in The Ethernet*)

Harjono

Teknik Informatika, F. Teknik, Universitas Muhammadiyah Purwokerto
Jl. Raya Dukuhwaluh PO. Box 202 Purwokerto 53182

harjono@ump.ac.id

Abstrak – Ethernet merupakan teknologi jaringan yang paling populer saat ini. Semua perangkat yang terhubung di dalam jaringan harus mengikuti aturan berupa protokol agar dapat berkomunikasi. Salah satu protokol yang ada pada *TCP/IP protocol suite* adalah *Address Resolution Protocol* (ARP). Fungsi dari ARP adalah menerjemahkan alamat logika menjadi alamat fisik. Penelitian ini bertujuan untuk menyimulasikan peran dari ARP dalam sebuah Ethernet menggunakan *Packet Tracer*. Proses resolusi alamat yang dilakukan oleh ARP, yang aslinya berlangsung sangat cepat dan tidak terlihat, dapat diamati secara rinci dan jelas dengan melakukan simulasi. Dalam simulasi terlihat komunikasi antar host dalam jaringan dapat dilakukan jika alamat fisik dari host tujuan sudah diketahui. Apabila alamat fisiknya belum diketahui maka ARP akan melaksanakan fungsinya.

Kata kunci: Ethernet, TCP/IP, ARP, simulasi, packet tracer.

Abstract - *Ethernet is the most popular network technology today. All devices connected within the network must follow protocols in order to communicate. One of the protocols in the TCP/IP protocol suites is the Address Resolution Protocol (ARP). The function of ARP is to translate logical addresses into physical addresses. This research aims to simulate the role of ARP in the Ethernet using Packet Tracer. The address resolution process performed by ARP, which originally took place very quickly and was not visible. It can be observed in detail and clearly by the simulation. In the simulation, communication between hosts in the network can be done if the physical address of the destination host is known. If the physical address is not known then ARP will perform its function.*

Keywords: Ethernet, TCP/IP, ARP, simulation, packet tracer.

I. PENDAHULUAN

Ethernet merupakan teknologi jaringan yang paling terkenal dan paling banyak digunakan di dunia saat ini. Dengan *Ethernet* kita bisa menghubungkan banyak komputer dengan biaya rendah dan fleksibilitas tinggi. Teknologi *Ethernet* dirancang untuk diterapkan pada berbagai lingkungan, mulai dari jaringan untuk rumah, kantor, kampus, dan jaringan lintas kota dan negara.

Ethernet digunakan untuk membangun jaringan dari yang terkecil sampai yang terbesar, dan dari yang paling sederhana sampai yang paling rumit. *Ethernet* digunakan untuk menghubungkan komputer di rumah dan perangkat rumah tangga lainnya, juga mendukung jaringan kabel yang menghubungkan server dan komputer desktop. Selain itu Ethernet juga menghubungkan akses point nirkabel dengan smartphone, laptop, dan tablet. Ethernet menyediakan koneksi yang membentuk internet di seluruh dunia [1].

Agar dapat berkomunikasi maka semua perangkat yang terhubung di dalam jaringan harus mengikuti aturan berupa protokol. Protokol yang digunakan untuk berkomunikasi di internet adalah *Transmission Control Protocol/Internet Protocol* (TCP/IP). Salah satu protokol yang ada diantara sekian banyak protokol pada *TCP/IP protocol suite* adalah *Address Resolution Protocol* (ARP). Tanggung jawab dari ARP dalam Ethernet adalah melakukan pemetaan antara alamat logika (*IP address*) dengan alamat fisik (*MAC address*) [2]. Sebuah frame Ethernet memerlukan alamat fisik tujuan agar berhasil dikirimkan. Sehingga peran dari ARP ini sangat penting.

Proses resolusi alamat yang dilakukan oleh ARP dalam jaringan berlangsung sangat cepat dan tidak terlihat sehingga sulit untuk diamati. Untuk melakukan analisis sebuah jaringan selain

menggunakan perangkat keras juga dapat dilakukan dengan memanfaatkan perangkat lunak simulasi. Salah satu perangkat lunak simulasi jaringan adalah Packet Tracer dari Cisco.

Terdapat banyak keuntungan yang didapat dari packet tracer. Konsep dasar jaringan komputer yang sulit dipahami secara teori akan menjadi lebih mudah jika menggunakan packet tracer. Packet tracer memiliki banyak fitur untuk membangun berbagai skenario jaringan. Seseorang akan lebih percaya diri ketika bekerja menggunakan peralatan jaringan riil jika sebelumnya sudah banyak berlatih dengan packet tracer [3].

Rancangan dan simulasi topologi jaringan telah dibuat oleh [4] menggunakan packet tracer. Berbagai topologi sudah diimplementasikan dengan beberapa konsep penting seperti DHCP dan DNS menggunakan Cisco Packet Tracer. Jaringan sederhana dengan router dan switch juga berhasil disimulasikan. Sementara itu [5] juga telah melakukan studi dan implementasi *Routing protocol* menggunakan Packet tracer.

II. METODE PENELITIAN

Perangkat lunak yang digunakan dalam penelitian ini berupa perangkat lunak Packet Tracer versi 7.0.0 yang diinstal pada sistem operasi Windows 7. Sedangkan peralatan yang digunakan berupa sebuah perangkat keras komputer dengan spesifikasi Processor Intel Core i5 (1,8 GHz), RAM 4 GB, Hardisk 500GB.

Penelitian diawali dengan melakukan analisis sistem berupa analisis kebutuhan hardware dan software. Langkah berikutnya dilakukan perancangan topologi jaringan. Setelah rancangan diimplementasikan dengan Packet Tracer serta dilakukan konfigurasi, maka tahap selanjutnya adalah simulasi. Pada simulasi ini akan memperlihatkan mekanisme kerja dari ARP.

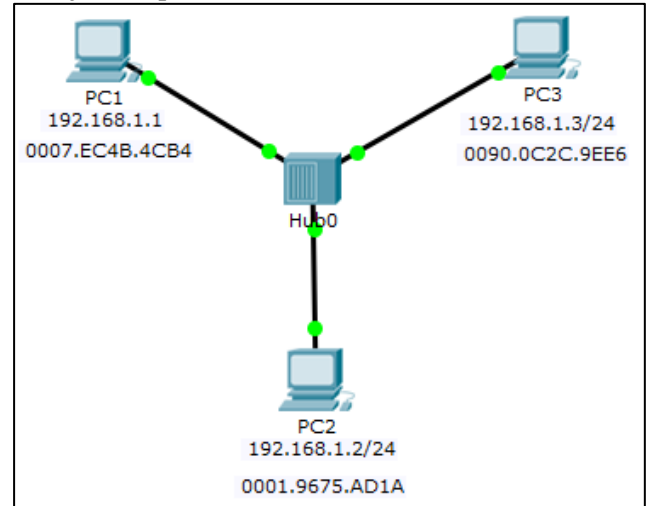
III. HASIL DAN PEMBAHASAN

A. Analisis Kebutuhan Sistem

Untuk dapat mengamati fungsi atau cara kerja dari ARP maka diperlukan sebuah simulasi dengan menggunakan aplikasi Packet Tracer yang diinstal pada sebuah komputer. Simulasi yang dilakukan harus dapat memperlihatkan setiap tahapan proses komunikasi antar host dalam jaringan, serta rincian dari *Protocol Data Unit* (PDU) dalam model *Open System Interconnection* (OSI).

B. Topologi Jaringan

Untuk bisa mengamati bagaimana ARP melaksanakan tugasnya dalam sebuah Ethernet, maka dibuat rancangan sebuah jaringan sederhana yang terdiri dari 3 buah komputer yang terhubung dengan sebuah Hub. Rancangan jaringan ditunjukkan pada Gambar 1.



Gambar 1. Diagram Topologi

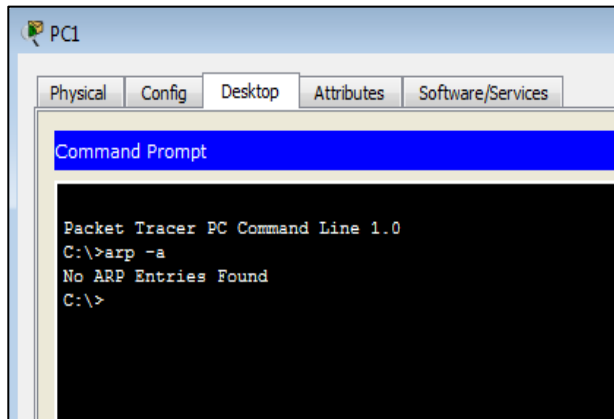
Jaringan dibuat menggunakan kelas C dengan alamat 192.168.1.0/24. Semua komputer kemudian dikonfigurasi dengan memberikan IP Address untuk PC1, PC2, dan PC3 berturut-turut 192.168.1.1, 192.168.1.2, dan 192.168.1.3. Sedangkan untuk alamat fisik atau MAC Address dari masing-masing komputer seperti tertampil pada Gambar 1.

C. Simulasi

Untuk mengamati bagaimana keterlibatan ARP serta mekanisme kerjanya dalam jaringan, maka digunakan sebuah skenario berupa komunikasi antara PC1 dan PC2. Komunikasi terjadi dengan memanfaatkan perintah *PING*. Perintah *PING* merupakan perintah yang dipergunakan untuk memeriksa koneksi antar host dalam jaringan yang menggunakan protokol TCP/IP.

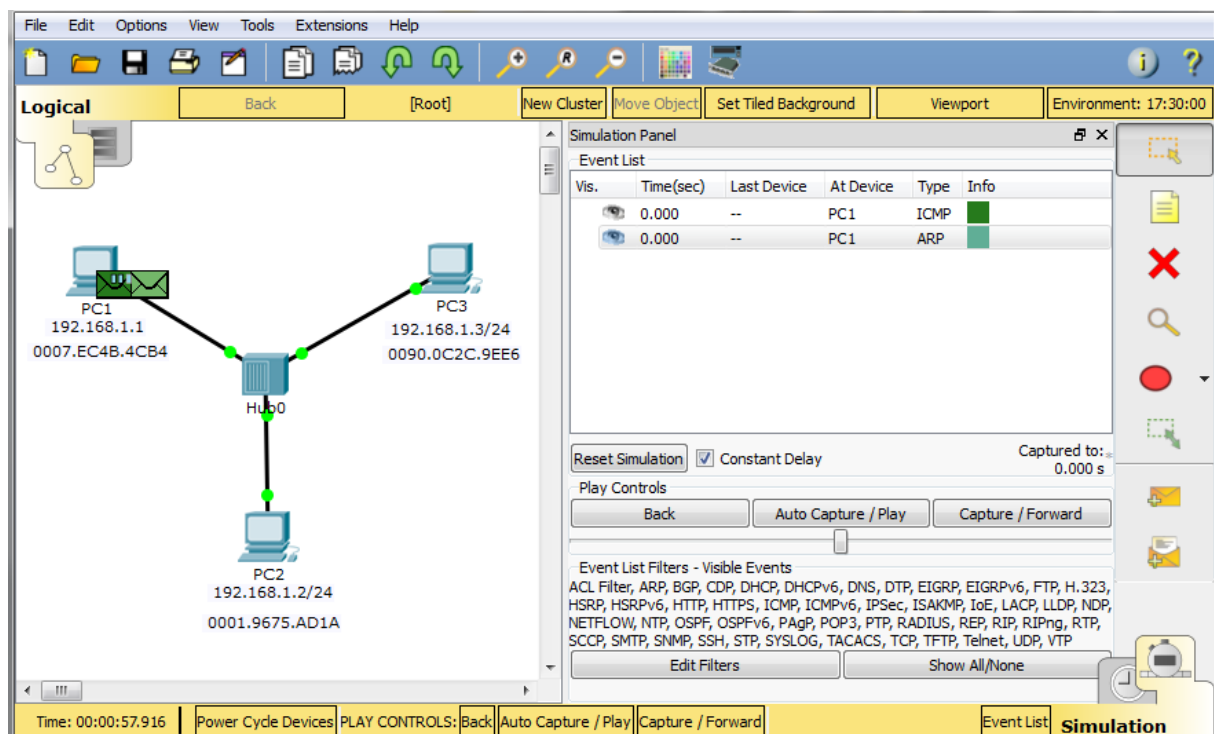
Menurut [2], ketika sebuah host akan mengirimkan IP packet ke host lain, pasti menyertakan IP address host tujuan tersebut. IP packet selanjutnya dienkapsulasi ke dalam bentuk frame Ethernet supaya dapat dikirimkan lewat jaringan fisik. Artinya host pengirim harus mengetahui alamat fisik (MAC address) dari host tujuan. Untuk memperoleh alamat fisik dari sebuah alamat logik (IP Address) merupakan tanggung jawab ARP. Informasi MAC address dari setiap IP address disimpan dalam ARP cache (tabel ARP) dari

host yang bersangkutan. Untuk melihat isi tabel ARP dengan menggunakan perintah **arp -a**. Gambar 2 menunjukkan tabel ARP dari PC1 masih kosong.



Gambar 2. ARP Cache PC1

Untuk menyimulasikan perintah PING tersebut dilakukan dengan menggunakan Traffic Generator dengan sumber PC1 dan tujuan PC2. Untuk mengamati traffic secara rinci maka Packet Tracer harus dijalankan dalam mode simulasi. Setiap tahapan dapat diamati dengan menggunakan tombol “Capture/Forward” pada ‘Simulation Panel’ seperti ditunjukkan pada Gambar 3.



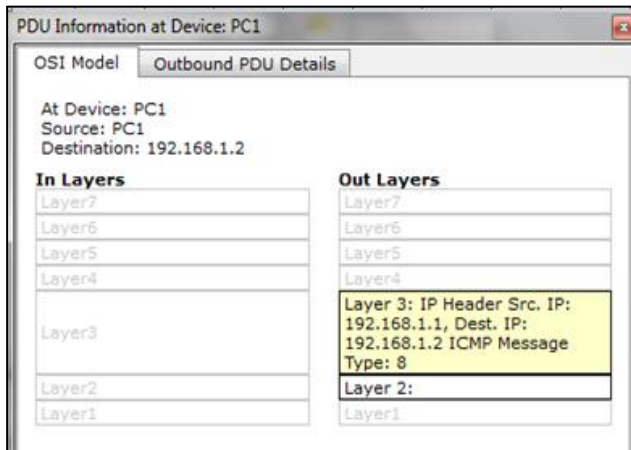
Gambar 3. Perintah Ping dengan Traffic Generator

Ketika perintah PING dijalankan dari PC1 menuju PC2 maka tampil 2 amplop sebagai representasi dari *Protocol Data Unit* (PDU) pada PC1 yaitu ARP packet dan ICMP packet. Perintah PING menghasilkan ICMP packet yang berupa pesan ICMP Echo Request dari IP sumber 192.186.1.1 ke tujuan 192.168.1.2. Gambaran ICMP packet dari OSI model seperti pada Gambar 4.

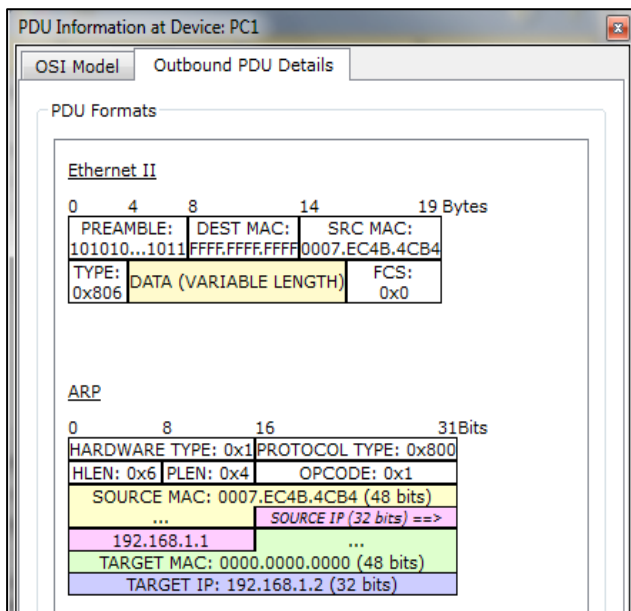
IP address tujuan adalah unicast yaitu 192.168.1.2 maka alamat tersebut dicari dalam Tabel

ARP. Karena tidak ditemukan dalam Tabel ARP maka PC1 membangkitkan ARP request untuk IP address tujuan 192.168.1.2. Pada tahap inilah ARP menjalankan fungsinya. Sementara itu ICMP packet disimpan dalam buffer sampai MAC address dari host tujuan didapatkan. PDU yang dibangkitkan dapat dilihat pada Gambar 5. Informasi penting yang ada pada ARP request adalah IP address tujuan yaitu 192.168.1.2 dan MAC address tujuan berisi 000.000.000 karena tidak diketahui. Jika dengan

bahasa kita maka ARP request tersebut berisi pesan IP address 192.168.1.2 mempunyai MAC address berapa?



Gambar 4. ICMP Packet dari PC1



Gambar 5. PDU dari ARP Request PC1

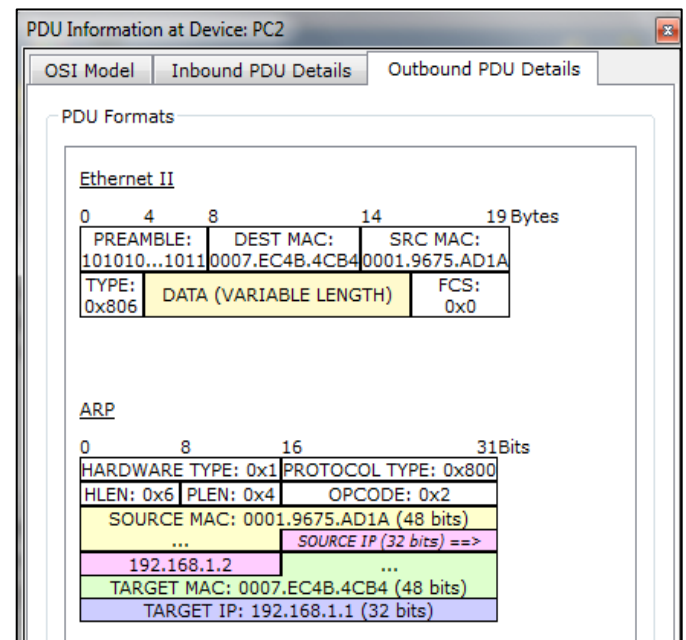
ARP request tersebut di layer 2 dienkapsulasi dalam sebuah frame Ethernet. Proses enkapsulasi dengan menambahkan header Preamble, Destination MAC Address, Source MAC Address, Type, dan Frame Check Sequence (FCS). Preamble menandai awal frame yang digunakan untuk sinkronisasi antara pengirim dan penerima. Destination MAC Address berupa alamat broadcast yaitu FFFF.FFFF.FFFF, sehingga frame ini akan dikirim ke seluruh host dalam jaringan. Pesan ARP memiliki Type 0x806, yang menginformasikan kepada penerima untuk meneruskan ke proses ARP.

Sedangkan field FCS digunakan untuk mendeteksi adanya kesalahan (*errors*).

Frame ini diteruskan ke layer 1, kemudian FastEthernet akan mengirimkan frame ke media transmisi. Oleh Hub, frame tersebut diteruskan ke semua port kecuali port dimana frame tersebut berasal. Host penerima yaitu PC2 dan PC3 menerima frame tersebut dan memrosesnya.

PC3 yang menerima frame yang berasal dari PC1 akan meneruskan frame dari layer 1 ke layer2. Kemudian dilakukan pengecekan MAC address tujuan yang berisi alamat broadcast, sehingga dilakukan dekapsulasi terhadap frame yang berisi ARP request tadi. IP address tujuan pada ARP request 192.168.1.2 ternyata berbeda dengan IP Address PC3 192.168.1.3, sehingga frame tersebut didrop.

Pada PC2 juga dilakukan proses serupa. Frame yang diterima juga didekapsulasi dan menghasilkan ARP request. IP address tujuan pada ARP request 192.168.1.2 dicocokkan dengan IP address PC2, ternyata sama. ARP kemudian melakukan update ARP cache. ARP kemudian membalas ARP request tadi dengan ARP reply. Pesan ARP reply berisi informasi IP address pengirim (192.168.1.2) dan MAC address pengirim (0001.9675.AD1A). ARP reply tersebut kemudian dienkapsulasi ke dalam sebuah frame Ethernet seperti pada Gambar 6. Header pada frame tersebut diantaranya adalah MAC address tujuan 0007.EC4B.4CB4 (PC1) dan MAC address sumber 0001.9675.AD1A (PC2).



Gambar 6. PDU dari ARP Reply PC2

Frame tersebut ditujukan kepada host dengan MAC address 0007.EC4B.4CB4 yaitu PC1. Frame yang merupakan ARP reply tersebut sebagai balasan atau jawaban terhadap ARP request dari PC1. Frame tersebut diteruskan oleh Hub ke semua port kecuali port tempat frame tersebut memasuki Hub. PC3 yang menerima frame tersebut membandingkan MAC address tujuan yang ada pada header frame tersebut dengan MAC addressnya. Karena tidak sama maka PC3 tahu bahwa frame tersebut bukan ditujukan padanya, sehingga frame tersebut didrop.

Sedangkan PC1 melihat MAC address tujuan pada header frame sama dengan MAC address miliknya. Sehingga PC1 tahu bahwa frame tersebut untuknya. Kemudian PC1 melakukan dekapsulasi terhadap frame Ethernet tersebut dan didapatkan ARP reply. Dengan informasi yang ada pada ARP reply inilah ARP melakukan update pada tabel ARP. Seperti terlihat pada Gambar 7, tabel ARP yang tadinya masih kosong kini sudah berisi IP address beserta MAC address dari PC2.

```

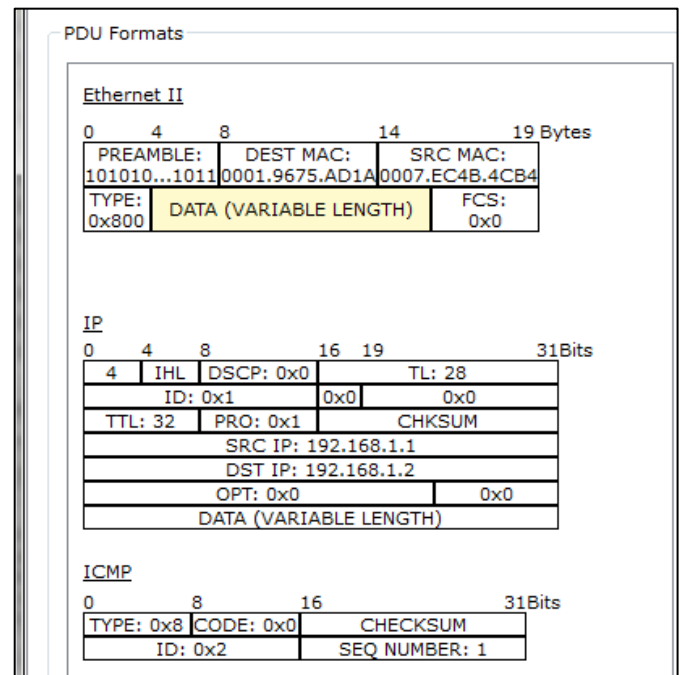
Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>arp -a
Internet Address      Physical Address      Type
192.168.1.2          0001.9675.ad1a       dynam

```

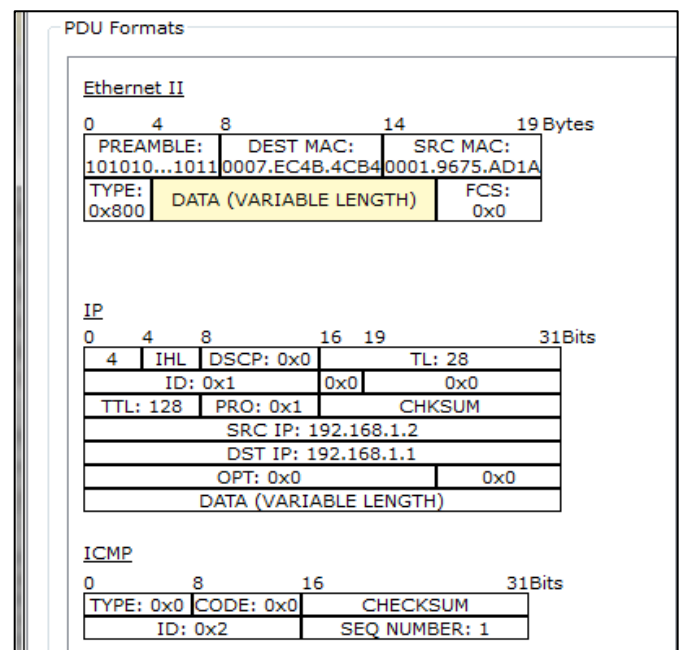
Gambar 7. Tabel ARP dari PC1 setelah diupdate

ICMP packet berupa pesan ICMP Echo Request yang sebelumnya tersimpan dalam buffer kemudian dikirim ulang dengan melakukan enkapsulasi terlebih dahulu. Header dari frame Ethernet ini berupa MAC address sumber 0007.EC4B.4CB4 dan MAC address tujuan 0001.9675.AD1A. Pada bagian Type bernilai 0x800 yang menunjukkan bahwa muatan dalam frame Ethernet tersebut adalah Internet Protocol (IP). Rincian dari PDU yang dikirimkan PC1 dapat dilihat pada Gambar 8.

PC2 yang merupakan tujuan dari frame yang berisi pesan ICMP Echo Request menerima frame tersebut dan mendekapsulasi frame tadi. Karena muatan dari frame tadi berupa pesan ICMP Echo Request, maka PC2 membalasnya dengan pesan ICMP Echo Reply. Pesan ini kemudian dienkapsulasi dalam sebuah frame Ethernet dengan header MAC address tujuan 0007.EC4B.4CB4 yang merupakan MAC address dari PC1 seperti pada Gambar 9.



Gambar 8. PDU ICMP Request dari PC1



Gambar 9. PDU ICMP Reply dari PC2

Frame dari PC2 yang berisi ICMP Reply tadi diteruskan oleh Hub ke semua port. PC1 yang memiliki MAC address sesuai dengan MAC address tujuan pada frame kemudian mengambil frame tadi dan mendekapsulasinya. Didapatkan muatan dari frame adalah ICMP Echo Reply dari PC2 sebagai balasan dari ICMP Echo Request yang dikirimkannya.

IV. PENUTUP

A. Kesimpulan

Dari hasil simulasi, dapat ditarik kesimpulan bahwa dalam sebuah Ethernet, ARP memiliki fungsi yang sangat penting yaitu menerjemahkan dari IP address ke MAC address yang sesuai. Proses enkapsulasi paket IP membutuhkan MAC address untuk membentuk sebuah frame Ethernet yang dapat dikirimkan. Selain itu ARP juga berfungsi memelihara ARP cache.

B. Saran

Dalam penelitian ini dilakukan simulasi pada komunikasi yang terjadi secara lokal atau dalam satu jaringan saja. Perlu dilakukan simulasi untuk komunikasi dengan remote host.

DAFTAR PUSTAKA

- [1] Spurgeon, C.E. and Zimmerman, J., 2014, *Ethernet: The Definitive Guide*, 2nd Edition, O'Reilly, California.
- [2] Forouzan, B.A., 2010, "TCP/IP Protocol Suite", Fourth Edition, Tata McGraw Hill.
- [3] Javid, S.R., 2014, Role of Packet Tracer in learning Computer Networks, *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 3, Issue 5, May 2014, ISSN 2319-5940.
- [4] Jain, G., noorani, N., Kiran, N., and Sharma, S., 2015, Designing & Simulation of Topology Network using Packet Tracer, *International Research Journal of Engineering and Technology (IRJET)*, Volume: 02 Issue: 02, May-2015, e-ISSN: 2395-0056.
- [5] Thrivikram, G., 2016, Configuring And Analysing of EIGRP Protocol using Cisco Packet Tracer, *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 4, Issue 3, March 2016, ISSN(Online): 2320-9801, ISSN print : 2320-9798.