Monitoring Protokol ARP Pada Wireshark

Moh.Lutfi Andrian
Lutfi9425@gmail.com
http://Andreyanlutfi.wordpress.com

Abstract

Open Systems Interconnection Model or OSI Model is a structural logic which organizing data communication on the network. This is purposed in order that computer can efficiently communicates on the different network.

There are 7 layer in the OSI Model. Every layer has particulary responsible on data communication process. OSI Model Layer divided into two group which are Upper Layer and Lower Layer. Upper Layer consists of Application, Presentation and Session. Then the Lower Layer consists of Transport, Network, Data Link and Physical.

The Address Resolution Protocol or ARP is a telecommunication protocol used for resolution of network layer addresses into link layer addresses, a critical function in multiple-access networks. ARP is used to convert an IP address into MAC address. ARP has been implemented with many combinations of network and data link layer technologies, such as IPv4, Chaosnet, DECnet and Xerox PARC Universal Packet (PUP) using IEEE 802 standards,

Keywords: OSI Model Layer, Application Layer, FTP.

Abstrak

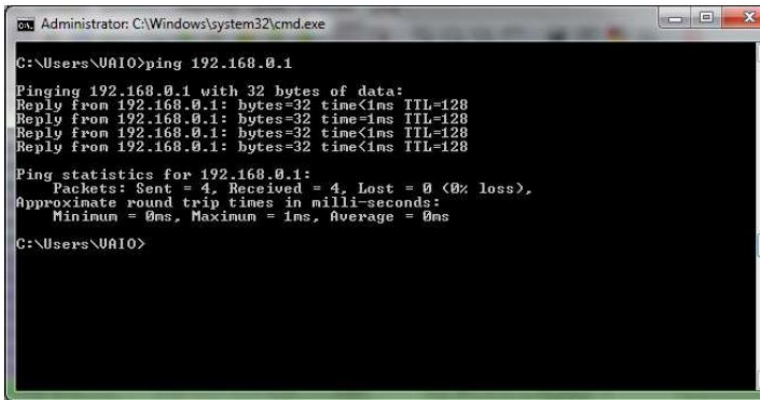
Open Systems Interconnection Model atau OSI Model merupakan kerangka logika terstruktur yang mengatur proses komunikasi data pada jaringan. Hal ini bertujuan agar komputer dapat berkomunikasi pada jaringan yang berbeda secara efisien.

Pada OSI model terdapat 7 Layer. Setiap Layer bertanggung jawab secara khusus pada proses komunikasi data. Model Layer OSI dibagi dalam dua group yaitu Upper Layer dan Lower Layer. Upper Layer terdiri dari Application, Presentation dan Session. Sedangkan Lower Layer terdiri dari Transport, Network, Data Link dan Physical.

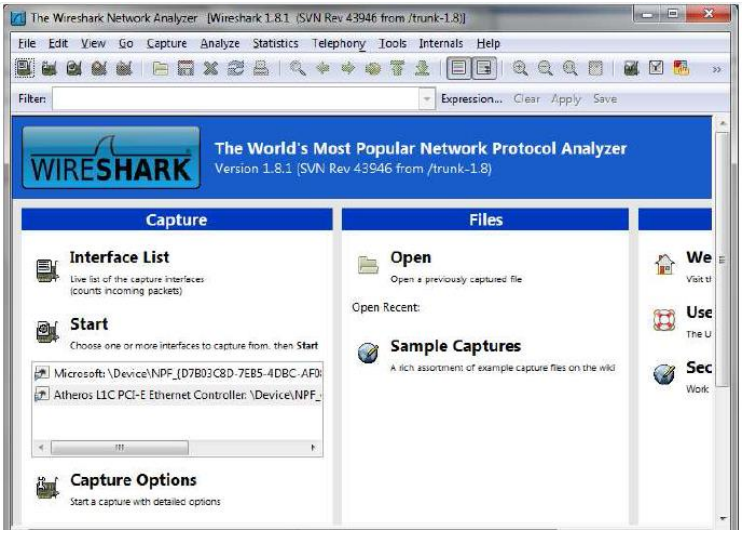
Address Resolution Protocol atau ARP adalah sebuah protokol dalam TCP/IP Protocol Suite yang bertugas melakukan resolusi alamat IP ke dalam alamat Media Access Control (MAC Address). ARP diimplementasikan dengan beberapa kombinasi dari teknologi network dan data link layer seperti Ipv4, Chaosnet, DECnet dan Xerox PARC Universal Packet (PUP) menggunakan standar IEEE 802.

Kata Kunci: OSI Model Layer, Application Layer, FTP

1. Pertama-tama hubungkan dua PC dengan kabel UTP Crossover.
2. Pastikan kedua PC sudah terhubung dengan baik dan benar dengan melakukan uji ping pada kedua PC.

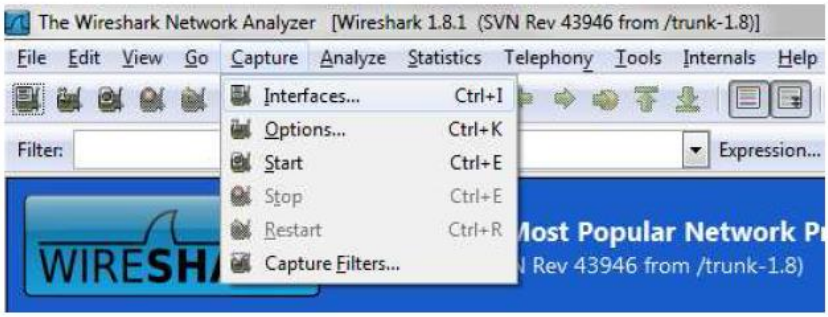


3. Lalu buka software wireshark yang sudah diinstal sebelumnya.



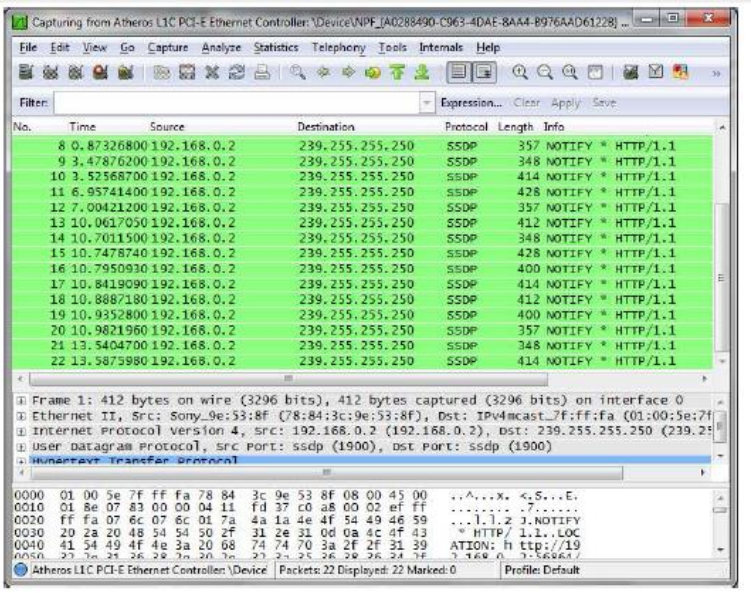
4. Lalu pilih pilihan Capture yang tersedia pada menu bar.

5. Selanjutnya pilih Interfaces atau tekan shortcut Ctrl+I

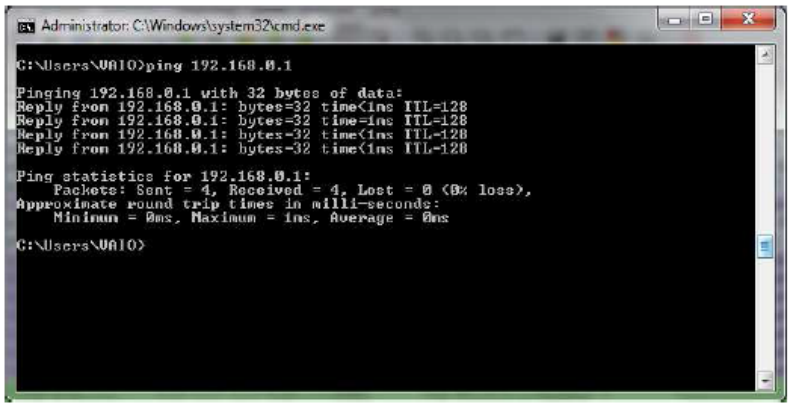


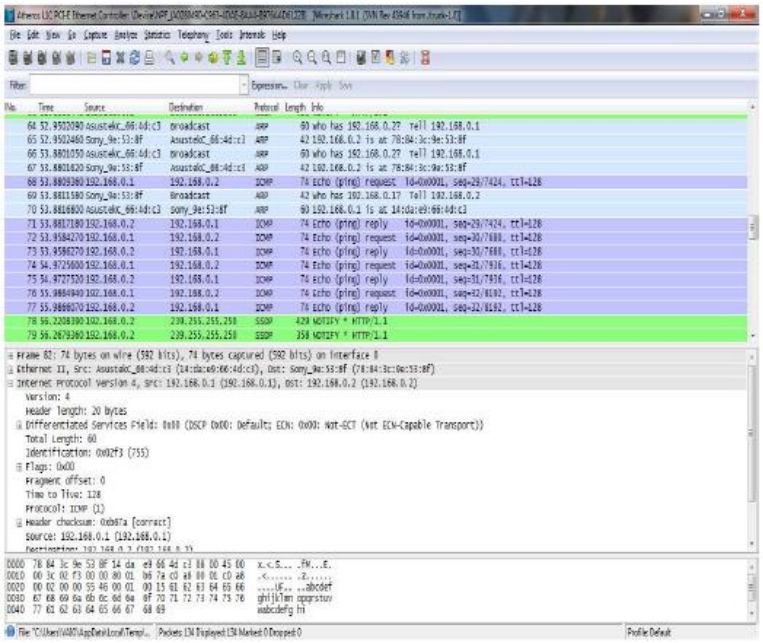
6. Setelah itu akan muncul interface yang tersedia. Pilih salah satu yang sedang berjalan dan terjadi transmisi paket data, pilih Start.

7. Setelah kita pilih salah satu interface maka akan muncul tampilan seperti di bawah ini.



8. Lalu lakukan tes ping. Akan muncul protokol ICMP dan ARP pada wireshark





9. Akan terlihat seperti gambar dibawah ini bahwa pada no. 64 source AsustekC_66:4d:c3 merupakan Mac Address PC yang melakukan ping, destination Broadcast karena mengirim keseluruh connection, Protocol ARP karena Mac Address belum mendapatkan Mac Address dari IP 192.168.0.2, info who has 192.168.0.2 tell 192.168.0.1 artinya siapakah pemilik IP 192.168.0.2 setelah diketahui pemiliknya maka akan diberi tahu ke IP 192.168.0.1 Kemudian pada no.65 source Sony_9e:53:8f merupakan Mac Address yang menjawab ke Mac Address pengirim yaitu pada destination AsustekC_66:4d:c3, Protocol ARP dengan membawa info 192.169.0.2 at 78:84:3c:9e:53:8f artinya sudah diketahui bahwa IP address 192.169.0.2 itu miliknya Mac Address 9e:53:8f. Setelah saling mengenal maka tampak protocol ICMP dan (ping) request, (ping) reply. Jadi sudah dapat saling mengenal kemudian dapat dilakukan connection untuk sharing data.

No.	Time	Source	Destination	Protocol	Length	Info
64	52.9502090	Asustekc_66:4d:c3	Broadcast	ARP	60	who has 192.168.0.2? Tell 192.168.0.1
65	52.9502460	Sony_9e:53:8f	Asustekc_66:4d:c3	ARP	42	192.168.0.2 is at 78:84:3c:9e:53:8f
66	53.8801050	Asustekc_66:4d:c3	Broadcast	ARP	60	Who has 192.168.0.2? Tell 192.168.0.1
67	53.8801620	Sony_9e:53:8f	Asustekc_66:4d:c3	ARP	42	192.168.0.2 is at 78:84:3c:9e:53:8f
68	53.8809360	192.168.0.1	192.168.0.2	ICMP	74	Echo (ping) request id=0x0001, seq=29/7424, ttl=128
69	53.8811580	Sony_9e:53:8f	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.2
70	53.8816800	Asustekc_66:4d:c3	Sony_9e:53:8f	ARP	60	192.168.0.1 is at 14:da:e9:66:4d:c3
71	53.8817180	192.168.0.2	192.168.0.1	ICMP	74	Echo (ping) reply id=0x0001, seq=29/7424, ttl=128
72	53.9584270	192.168.0.1	192.168.0.2	ICMP	74	Echo (ping) request id=0x0001, seq=30/7680, ttl=128
73	53.9586270	192.168.0.2	192.168.0.1	ICMP	74	Echo (ping) reply id=0x0001, seq=30/7680, ttl=128
74	54.9725600	192.168.0.1	192.168.0.2	ICMP	74	Echo (ping) request id=0x0001, seq=31/7936, ttl=128
75	54.9727520	192.168.0.2	192.168.0.1	ICMP	74	Echo (ping) reply id=0x0001, seq=31/7936, ttl=128
76	55.9864940	192.168.0.1	192.168.0.2	ICMP	74	Echo (ping) request id=0x0001, seq=32/8192, ttl=128
77	55.9866070	192.168.0.2	192.168.0.1	ICMP	74	Echo (ping) reply id=0x0001, seq=32/8192, ttl=128
78	56.2208390	192.168.0.2	239.255.255.250	SSDP	429	NOTIFY * HTTP/1.1

10. Kemudian jika di klik pada no.64 maka pada Ethernet II, Source AsustekC_66:4d:c3 (14:da:e9:66:4d:c3) merupakan Mac Address pengirim, Dst: Broadcast (ff:ff:ff:ff:ff:ff) artinya bahwa tujuan ke semua Mac Address yang memiliki IP Address yang dituju. Kemudian Address Resolution Protocol (request) tampak seperti gambar dibawah ini. Lihat di sender MAC Address

: AsustekC_66:4d:c3 (14:da:e9:66:4d:c3) dengan memiliki IP Address 192.168.0.1 (192.168.0.1) dan target MAC Address : 00:00:00_00:00:00 (00:00:00:00:00:00) dengan IP targetnya 192.168.0.2 (192.168.0.2) artinya bahwa pemilik IP Address 192.168.0.2 belum diketahui MAC Address nya maka target MAC Address nya 00:00:00_00:00:00 (00:00:00:00:00:00). Dan protocol type IP itu 800.

Penutup

Jadi sebelum mengenal antara PC atau jika PC pengirim belum mengetahui MAC Address dari yang dituju maka PC pengirim akan mengirim ARP dan ARP disini
fungsinya untuk pendataan siapa pemillik dari IP Address yang dituju. Setelah mengetahui bahwa misalnya dalam praktikum ini MAC Address yang dituju diketahui Sony_9e:53:8f maka ARP disini akan membuat tabel yang menyatakan bahwa IP Address 192.168.0.2 milik MAC Address Sony_9e:53:8f dan aka dilakukan proses maping ARP sebelum mengenal IP Address dengan MAC Address yang dituju setelah mengenal maka ARP tidak digunakan karena pada ARP telah membuat tabel dengan melihat data yang telah di map ARP. Kemudian setelah saling mengenal maka hanya mengirim request pada protocol ICMP dan dibalas/reply pada protocol ICMP.

Referensi

Kurniawan A, *Network Forensics: Panduan Analisis Dan Investigasi Paket Data Jaringan Menggunakan Wireshark*. Yogyakarta: Andi. 2012

Biografi Penulis

Moh.Lutfi andrian.Lahir di jepara 20 nopember 1994.Menyelesaikan diSMA Walisongo jepara tahun 2011 .Sedang melaksanakan kuliah jenjang Sarjana di POLITEKNIK NEGERI SEMARANG angkatan 2011,Jurusan Elektro,Progam studi D4 telekomunikasi.