Simulasi dan Monitoring Protokol Dalam Tes Koneksi

Imam Prasetyo
imp.masiv@gmail.com
http://superman-kartini.blogspot.com

Pendahuluan

Pada dasarnya ada dua jenis metode yang digunakan untuk monitoring jaringan komputer, yaitu connection monitoring atau tes koneksi dan traffic monitoring. Keduanya memiliki hakikat yang sama yaitu proses pengumpulan dan melakukan analisis terhadap data-data pada lalu lintas jaringan dengan tujuan memaksimalkan seluruh sumber daya yang dimiliki Jaringan Komputer. Berikut ini penjelasan singkat mengenai kedua metode tersebut.

- Connection Monitoring

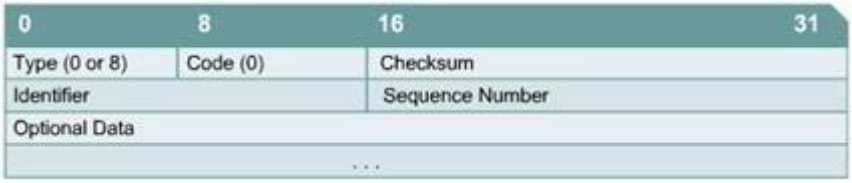
  Connection monitoring adalah teknik monitoring jaringan yang dapat dilakukan dengan melakukan tes koneksi atau ping antara monitoring station dan device target, sehingga dapat diketahui bila koneksi terputus.
- Traffic Monitoring

  Traffic monitoring adalah teknik monitoring jaringan dengan melihat paket aktual dari traffic pada jaringan dan menghasilkan laporan berdasarkan traffic jaringan.

Tes koneksi atau “ping” ini pada dasarnya bekerja pada layer aplikasi. Namun dalam prosesnya digunakan **Internet Control Message Protocol** (**ICMP**) yang mengirim pesan

ICMP *Echo Request*(dan menerima *Echo Reply*) untuk menentukan apakah komputer tujuan dapat dijangkau dan berapa lama paket yang dikirimkan dibalas oleh komputer tujuan.

Versi ICMP ini juga dikenal sebagai **ICMPv4**, yang merupakan bagian dari Internet Protocol versi 4. Sedangkan versi terkini yaitu ICMPv6. Berikut ini merupakan format header dari ICMPv4.



0	8	16	31
Type (0 or 8)	Code (0)	Checksum	
Identifier		Sequence Number	
Optional Data			
...			

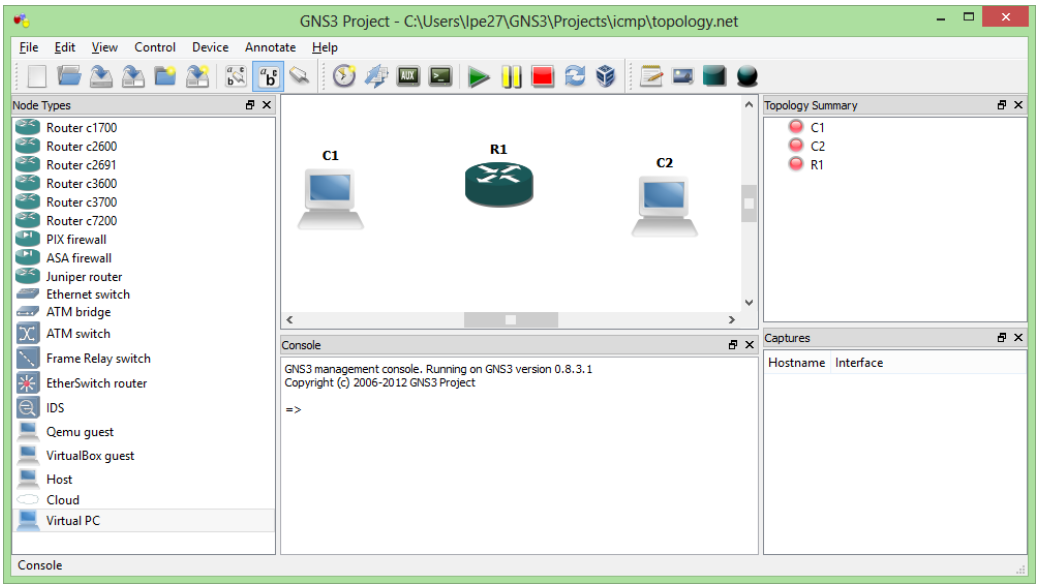
Tipe yang cocok dan nomor kode ditunjukkan di tiap-tiap tipe pesan. Field identitas dan field sequence number sifatnya unik untuk pesan echo request dan echo reply. Field-field itu digunakan mencocokkan echo reply dengan echo request. Field data berisi informasi tambahan yang mungkin bagian dari echo reply atau echo request. Berikut ini merupakan tipe dari pesan ICMP.

ICMP Message Types	
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect/ Change Request
8	Echo Request
9	Router Advertisement
10	Router Selection
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

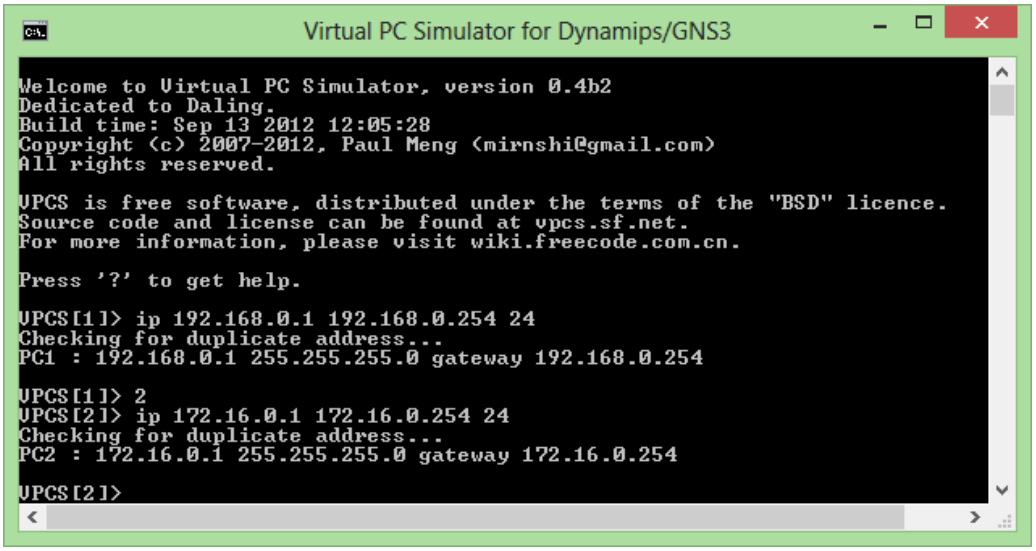
Simulasi Tes Koneksi dengan GNS3

Sebenarnya ada banyak cara untuk melakukan tes koneksi atau ping dalam suatu jaringan komputer baik real maupun virtual. Disini saya akan menggunakan aplikasi GNS3+VMWare untuk membuat suatu jaringan komputer virtual, kemudian akan melakukan tes koneksi (monitoring) terhadapnya. Berikut ini adalah langkah-langkahnya.

1. Membuka aplikasi GNS3 kemudian membuat jaringan komputer seperti gambar dibawah.

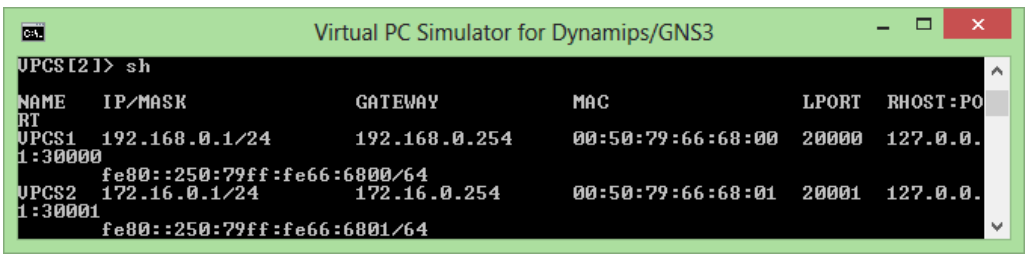


2. Bukalah VPCS.exe dan konfigurasi IP address dari masing masing PC.



Command : **ip <PC IP address> <IP Gateway> <mask>**

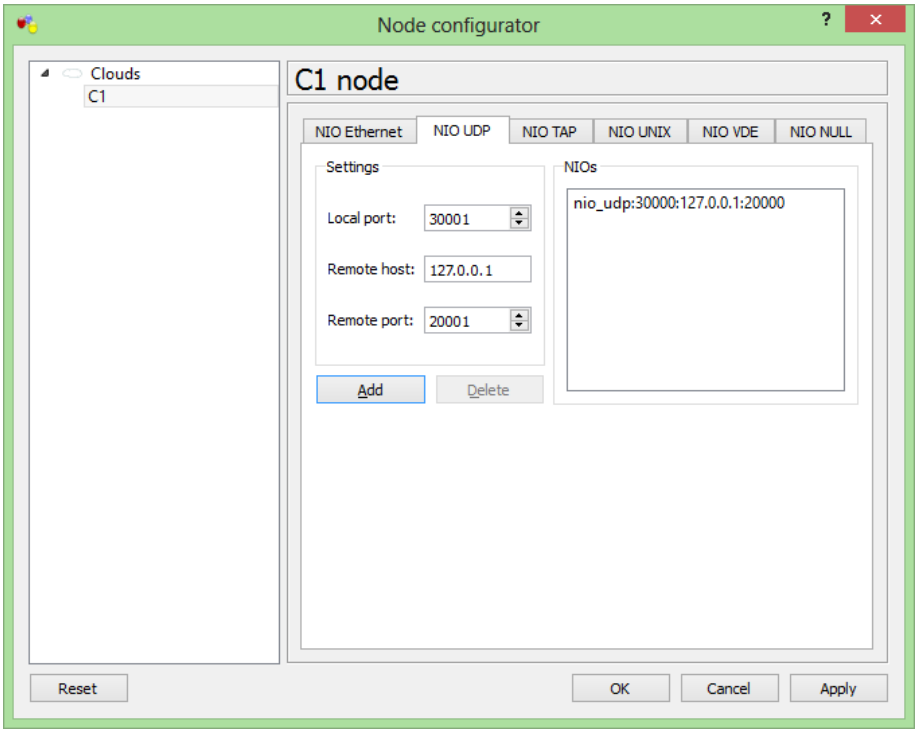
3. Ketikkan command "sh" pada VPCS.exe sehingga muncul data (LPORT dan RPORT) sebagai berikut yang akan digunakan untuk langkah berikutnya.



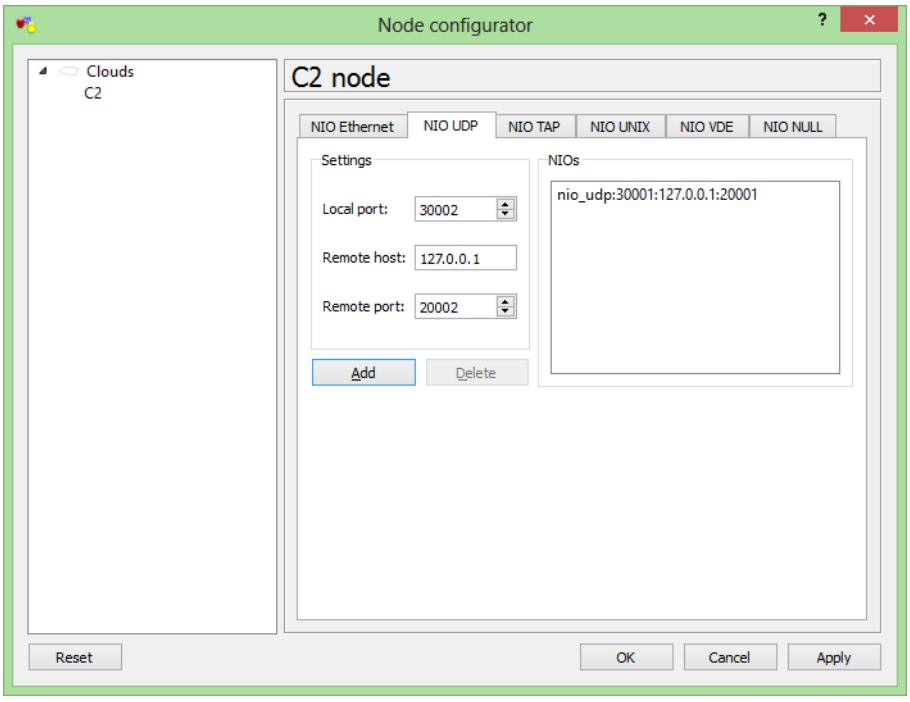
4. Mengkonfigurasi interface "NIO UDP" PC agar dapat dihubungkan dengan

VPCS.exe sehingga dapat digunakan untuk simulasi.

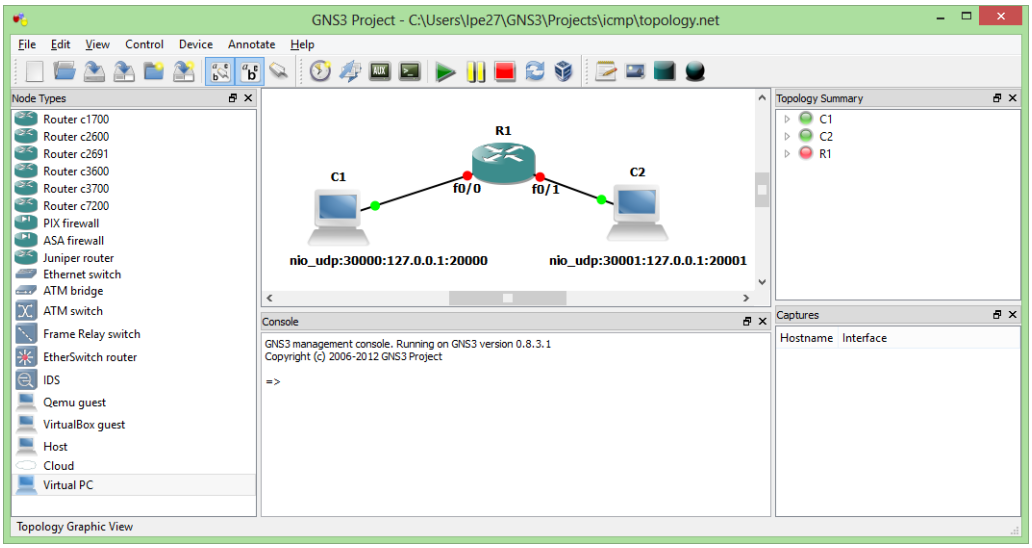
C1 (Komputer 1) → localport dan remoteport antara konfigurasi dan data vpcs.exe adalah kebalikan.



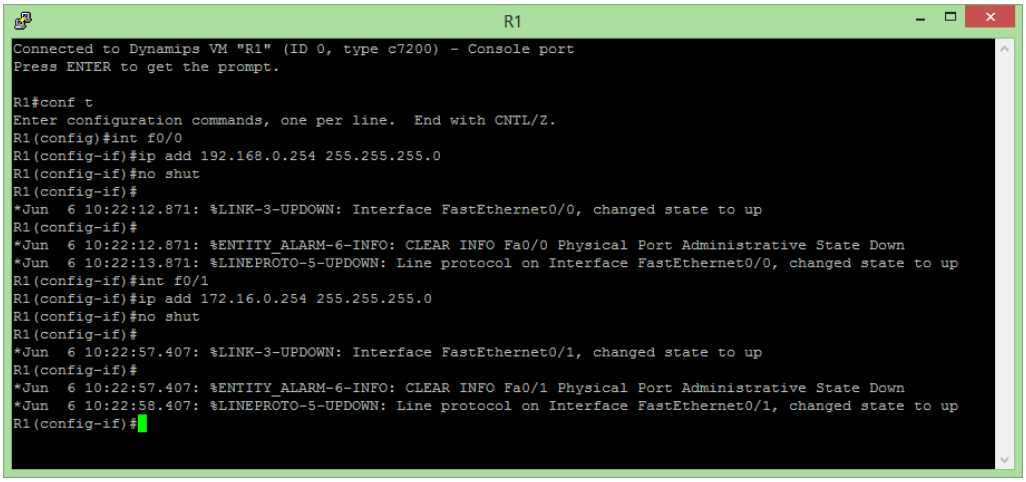
C2 (Komputer 2) → localport dan remoteport antara konfigurasi dan data vpcs.exe adalah kebalikan.



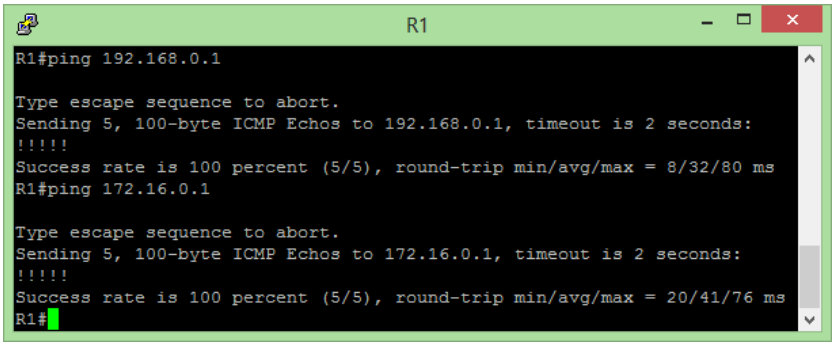
5. Hubungkan router dengan PC (pada interface NIO UDP yang dikonfigurasi tadi) menggunakan fastethernet seperti gambar berikut.



6. Konfigurasi router agar dapat menghubungkan segmen network yang berbeda (C1 dan C2)



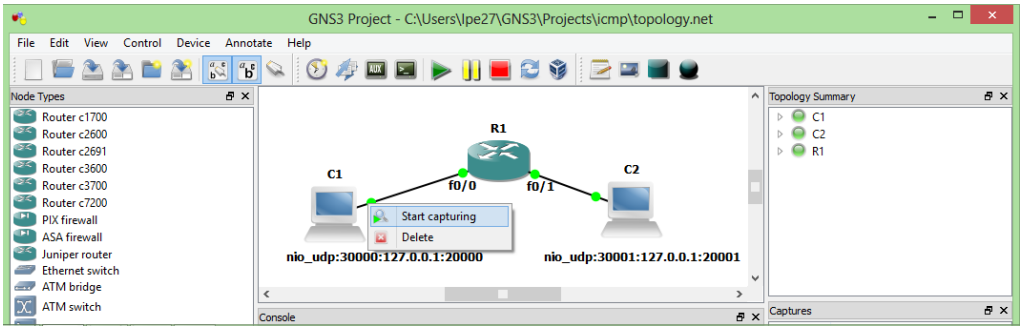
7. Jaringan Virtual telah berhasil dibuat. Langkah berikutnya adalah melakukan tes koneksi apakah jaringan benar-benar berjalan semestinya atau tidak. Berikut ini sample tes koneksi dari router ke kedua PC.



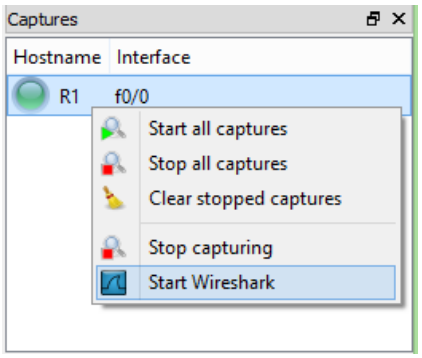
Monitoring Jaringan (Tes Koneksi dengan "Ping")

Monitoring yang akan dilakukan adalah menggunakan tools wireshark yang sebenarnya secara bundled ada bersama GNS3 all in one. Berikut ini adalah langkah-langkah dan analisisnya.

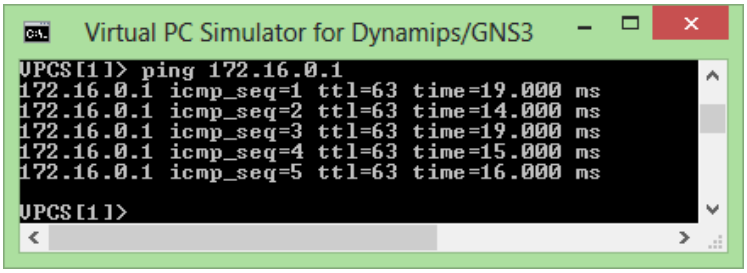
1. Pada jaringan virtual tadi klik kanan pada salah satu koneksi interface kemudian pilih "start capture". Disini saya mengcapture pada interface C1.



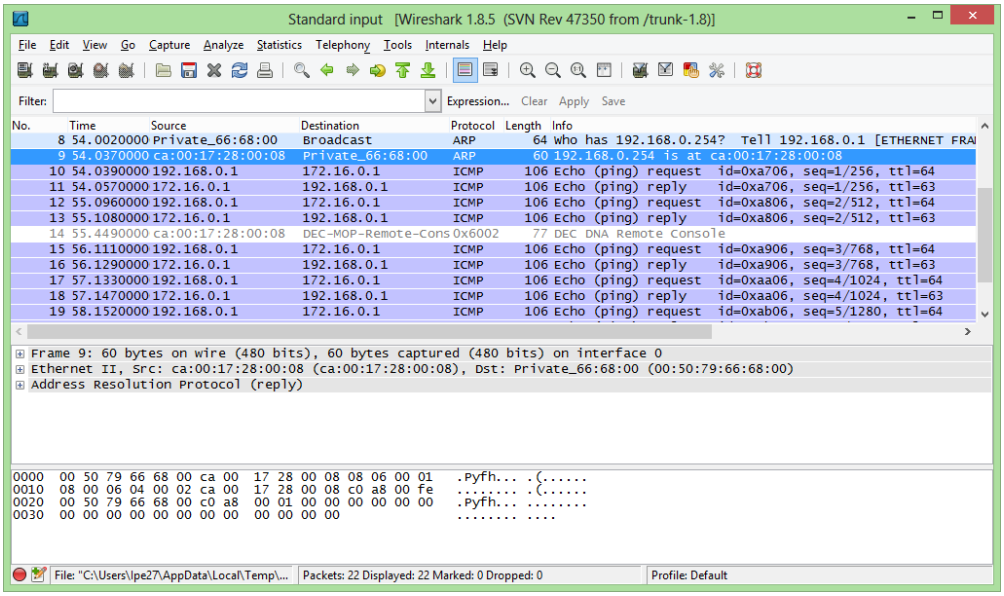
2. Pada menu capture klik "start wireshark"



3. Dari VPCS.exe, pada VPCS1 atau C1 (192.168.0.1) lakukan ping ke alamat C2 (172.16.0.1).

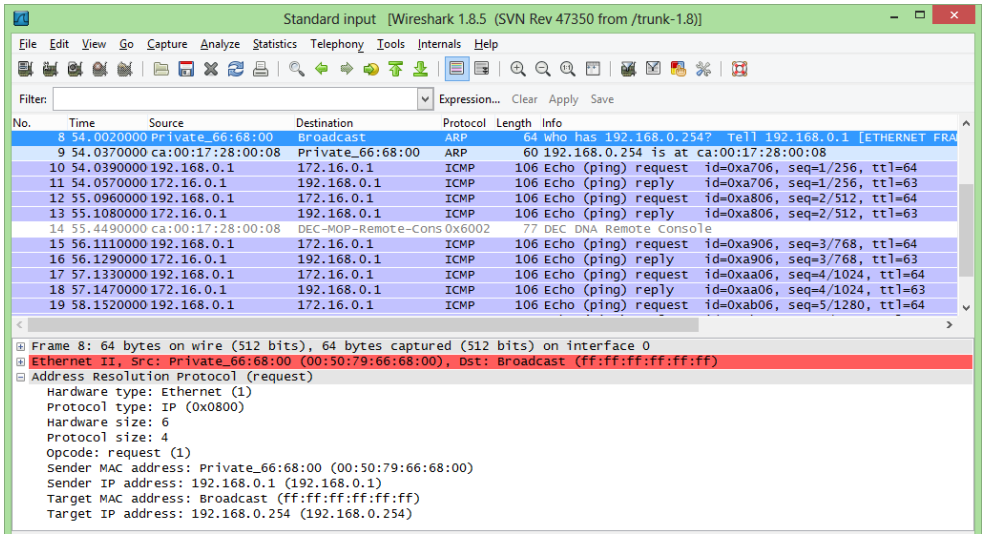


4. Maka pada wireshark akan tercapture proses ping yang kita lakukan tadi.



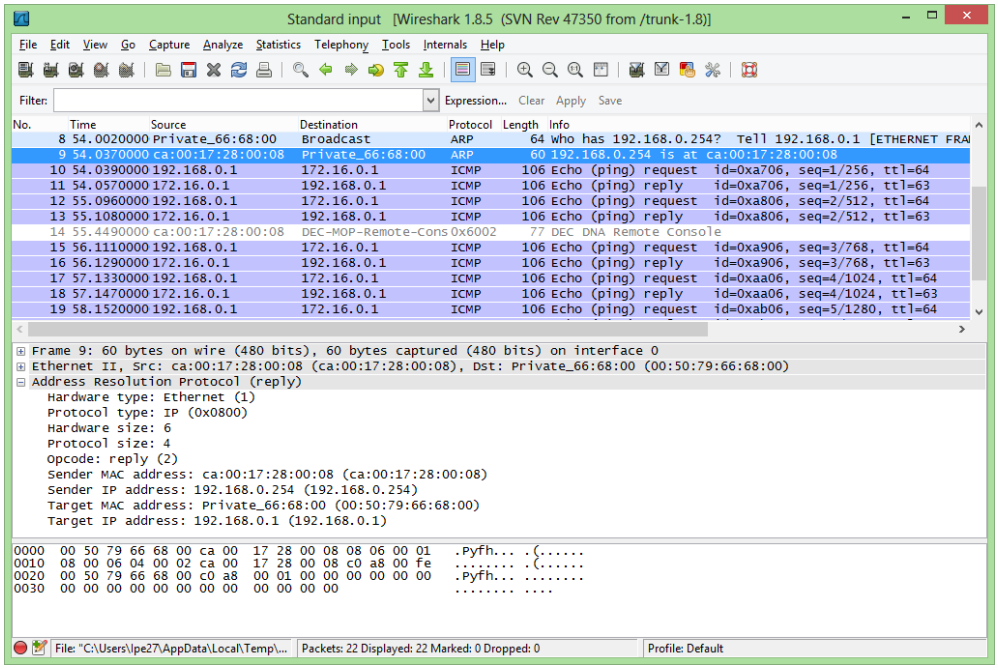
Dapat dilihat bahwa proses ping tadi melibatkan dua jenis protokol yaitu ARP (Address Resolution Protocol) dan ICMP (Internet Control Message Protocol). Protokol ARP itu sendiri digunakan untuk mengetahui alamat fisik dari hop berikutnya yang dituju yang notabennya alamat logikanya (IP address) diketahui. ARP dan ICMP sama sama bekerja di layer 3 atau network layer. Karena proses ping yang dilakukan adalah pertama kali (belum ada ARP cache) maka C1 tidak mengetahui alamat fisik dari hop berikutnya menuju tujuan sehingga dibutuhkan protokol ARP. Kemudian pesan echo ICMP dikirim dan diterima kembali oleh host sumber yang berarti koneksi berjalan baik.

- Proses ARP



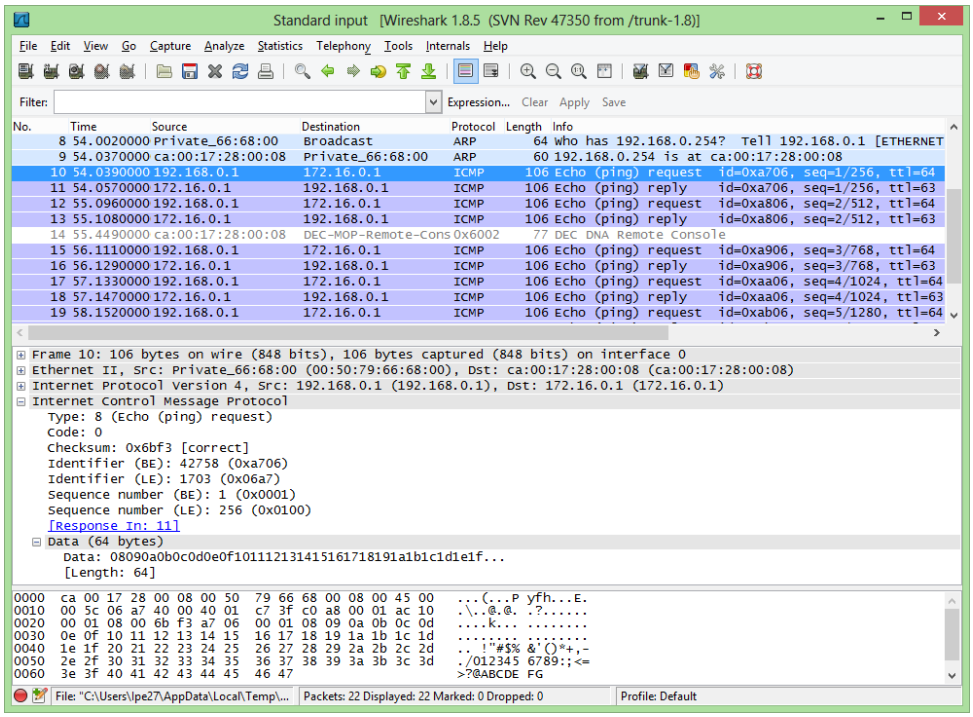
Pesan pertama adalah ARP request dari C1 (192.168.0.1) ke alamat broadcast

untuk mengetahui MAC address hop berikutnya (gateway R1 : 192.168.0.254).



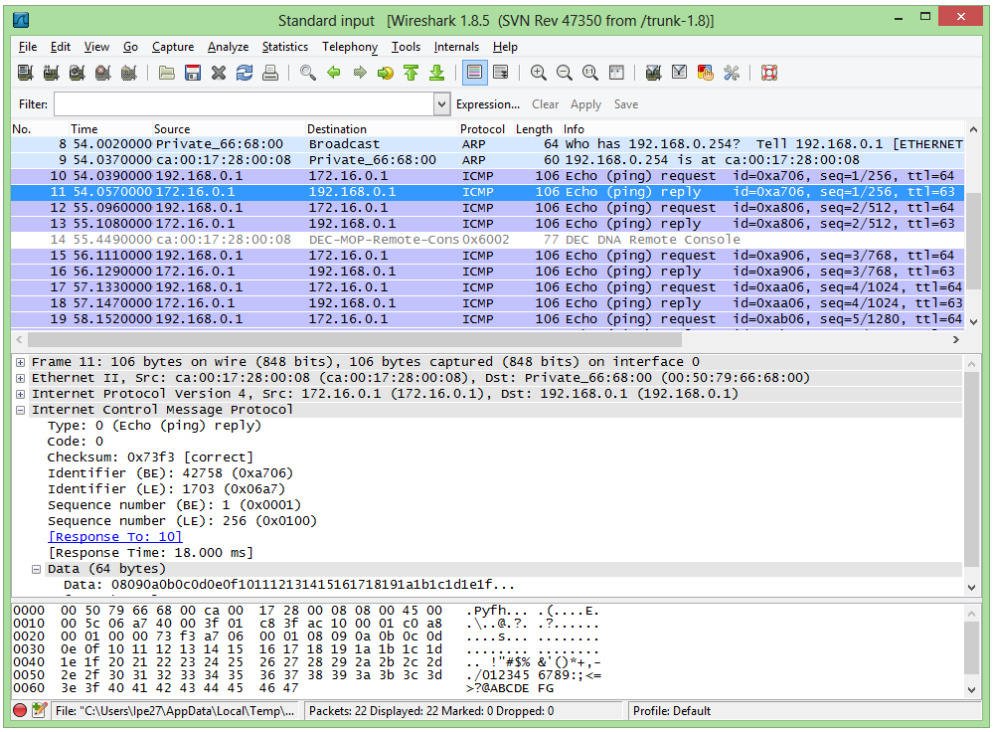
Pesan kedua adalah ARP reply yaitu dari R1 ke C1 yang isinya memberitahu bahwa hop berikutnya, IP 192.168.0.254 memiliki alamat fisik ca:00:17:28:00:08.

- Proses ICMP



Pada dasarnya proses ping itu sendiri adalah mengirimkan beberapa paket echo ICMP dan paket tersebut akan kembali lagi ke sumber yang

mengindikasikan suatu koneksi berjalan semestinya. Dapat dilihat pada frame 10 yaitu pesan ICMP pertama, tipenya adalah request. Tipe ini juga dapat diidentifikasi dari nilai Type yaitu 8 dan Code yaitu 0. Pesan ini dikirim oleh C1 (IP : 192.168.0.1) ke C2 (172.16.0.1).



Pesan ICMP kedua pada frame 11 adalah reply yaitu merupakan balasan dari C2 (IP : 172.16.0.1) bahwa echo ICMP dari C1 (192.168.0.1) telah sampai dan dikembalikan kepadanya. Disini juga dapat dilihat berapa waktu yang digunakan dalam perjalanan paket echo ICMP tadi yaitu pada response time : 18.000 ms.

Dapat dilihat kemudian pesan yang sama (ICMP request) dilakukan secara berulang dan mendapatkan balasan dari host tujuan berupa ICMP reply hingga proses ping selesai. Hal ini mengindikasikan koneksi berjalan semestinya atau C1 dan C2 terhubung dengan baik.

Topology GNS3 yang telah saya buat diatas dapat anda download di → http://www.mediafire.com/?7zq62we571wsccu

Biografi Penulis

Imam Prasetyo. Kuliah D4 Teknik Telekomunikasi di Politeknik Negeri Semarang. Lulusan SMA Negeri 1 Pati tahun 2010 dan SMP Negeri 1 Pati tahun 2007. Dari kecil sangat tertarik pada ilmu pengetahuan alam dan teknologi. Untuk informasi maupun tulisan menarik lain dapat diakses di situs blog *http://www.superman-kartini.blogspot.com*