

Monitoring Protokol ICMP menggunakan Wireshark

Annisa Cahyaningtyas

annisacahyaningtyas@gmail.com

http://annisacahyaningtyas.blogspot.com

Lisensi Dokumen:

Copyright © 2003-2007 IlmuKomputer.Com

Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

1. Internet Control Message Protocol (ICMP)

Internet Control Message Protocol (ICMP) adalah salah satu protokol inti dari protokol internet. ICMP utamanya digunakan oleh sistem operasi komputer jaringan untuk mengirim pesan kesalahan yang menyatakan, sebagai contoh, bahwa komputer tujuan tidak bisa dijangkau.

ICMP berbeda tujuan dengan TCP dan UDP dalam hal ICMP tidak digunakan secara langsung oleh aplikasi jaringan milik pengguna. salah satu pengecualian adalah aplikasi ping 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.

Internet Control Message Protocol (ICMP) adalah protokol yang digunakan untuk membantu error handling dan prosedur pengaturan (control procedure). Protokol ini bekerja pada network layer dan berurusan dengan layanan koneksi (connection services). Tugas dari ICMP adalah menyediakan *error control* dan *flow control* pada network layer.

Kegiatan yang berjalan di Internet dimonitor secara teliti oleh router. Jika terjadi sesuatu yang tidak diinginkan, kejadian tersebut akan dilaporkan oleh ICMP. ICMP mendeteksi kondisi error seperti kongesti/kemacetan internetwork (*internetwork congestion*) dan hubungan yang putus, lalu memberitahukan IP (Internet Protocol) dan protokol pada layer atas sehingga paket-paket dapat dikirimkan disekeliling area yang bermasalah.

Pesan/paket ICMP dikirim jika terjadi masalah pada layer IP dan layer atasnya (TCP/UDP). Pada kondisi normal, protokol IP berjalan dengan baik. Namun ada beberapa kondisi dimana koneksi IP terganggu, misalnya karena Router crash, putusnya kabel, atau matinya host tujuan. Pada saat ini ICMP membantu menstabilkan kondisi jaringan, dengan memberikan pesan-pesan tertentu sebagai respons atas kondisi tertentu yang terjadi pada jaringan tersebut.

2. Tipe Pesan ICMP

Ada dua tipe pesan yang dapat dihasilkan ICMP :

- a. ICMP Error Message (dihasilkan jika terjadi kesalahan jaringan)
- b. ICMP Query Message (dihasilkan jika pengirim paket mengirimkan informasi tertentu yang berkaitan dengan kondisi jaringan).

ICMP Error Message dibagi menjadi beberapa jenis :

1. Destination Unreachable, dihasilkan oleh router jika pengirim paket mengalami kegagalan akibat masalah putusnya jalur baik secara fisik maupun logic. Destination Unreachable dibagi lagi menjadi beberapa jenis :
 - a) Network Unreachable, jika jaringan tujuan tak dapat dihubungi
 - b) Host Unreachable, jika host tujuan tak bisa dihubungi
 - c) Protocol At Destination is Unreachable, jika di tujuan tak tersedia protokol tersebut.
 - d) Destination Host is Unknown, jika host tujuan tidak diketahui
 - e) Destination Network is Unknown, jika network tujuan tidak diketahui
2. Time Exceeded, dikirimkan jika isi field TTL dalam paket IP sudah habis dan paket belum juga sampai ke tujuannya. Tiap kali sebuah paket IP melewati satu router, nilai TTL dalam paket tsb, dikurangi satu. TTL ini diterapkan untuk mencegah timbulnya paket IP yang terus menerus berputar-putar di network karena suatu kesalahan tertentu. sehingga menghabiskan sumber daya yang ada.

Field TTL juga digunakan oleh program traceroute untuk melacak jalannya paket dari satu host ke host lain. Program traceroute dapat melakukan pelacakan rute berjalannya IP dengan cara mengirimkan paket kecil UDP ke IP tujuan, dengan TTL yang di set membesar.

Saat paket pertama dikirim, TTL diset satu, sehingga router pertama akan membuang paket ini dan mengirimkan paket ICMP Time Exceeded, kemudian paket kedua dikirim, dengan TTL dinaikan. Dengan naiknya TTL paket ini sukses melewati router pertama namun dibuang oleh router kedua, router ini pun mengirim paket ICMP time Exceeded.

3. Parameter Problem, paket ini dikirim jika terdapat kesalahan parameter pada header paket IP.
4. Source Quench, Paket ICMP ini dikirimkan jika router tujuan mengalami kongesti. Sebagai respons atas paket ini pihak pengirim paket harus memperlambat pengiriman paketnya.
5. Redirect, paket ini dikirimkan jika router merasa host mengirimkan paket IP melalui router yang salah. Paket ini seharusnya dikirimkan melalui router lain.

Sedangkan ICMP Query Message Terdiri atas :

1. Echo dan Echo Reply, Bertujuan untuk memeriksa apakah sistem tujuan dalam keadaan aktif. Program ping merupakan program pengisi paket ini. Respondet harus mengembalikan data yang sama dengan data yang dikirimkan.
2. Timestamp dan Timestamp Reply, Menghasilkan informasi waktu yang diperlukan sistem tujuan untuk memproses suatu paket.
3. Address mask, untuk mengetahui beberapa netmask yang harus digunakan suatu host dalam suatu network.

Sebagai paket pengatur kelancaran jaringan paket ICMP tidak diperbolehkan membebani network. Karenanya paket ICMP tidak boleh dikirim saat terjadi problem yang disebabkan oleh :

- a. Kegagalan pengiriman paket ICMP
- b. Kegagalan pengiriman paket broadcast atau multicast.

ICMP merupakan sebuah protokol manajemen dan penyedia layanan messaging untuk IP. ICMP berfungsi untuk melaporkan jika terjadi suatu masalah dalam pengiriman data. Berbagai hal yang dilaporkan adalah:

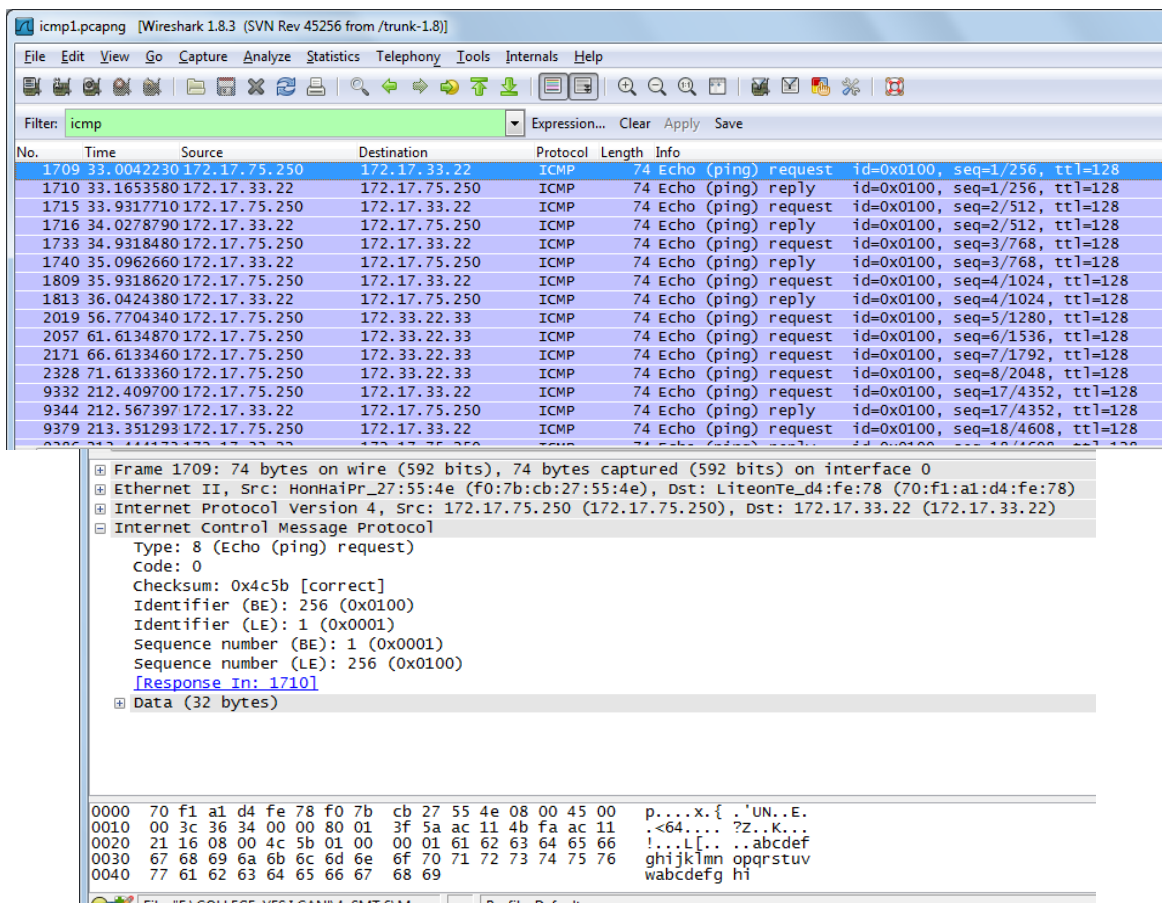
- a. Destination Unreachable, merupakan laporan yang mengindikasikan bahwa tujuan tidak dapat dijangkau.

- b. Buffer Bull, memberitahukan kepada pengirim jika memori penuh.
- c. Hops, memberitahu pengirim bahwa paket telah melalui jumlah hop maksimum dan akan diabaikan.
- d. Ping, menggunakan ICMP echo untuk memeriksa hubungan.

3. Monitoring ICMP menggunakan Wireshark

Dapat pula memonitoring protokol ICMP menggunakan Wireshark. Sebelumnya, kita sudah terhubung ke dalam suatu jaringan kemudian mengaktifkan terlebih dahulu aplikasi Wireshark lalu memilih Interfaces yang aktif kemudian dapat menuliskan ICMP pada kotak filter.

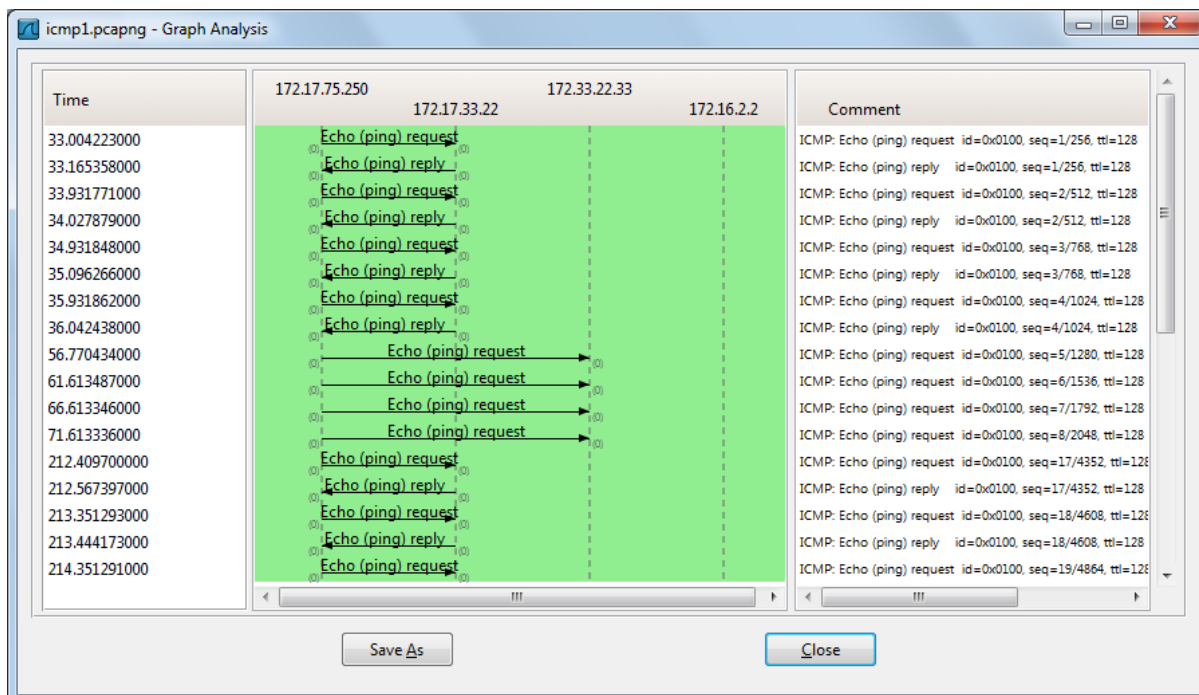
- a. Tampilan Wireshark saat melakukan monitoring ICMP yang berhasil, hal tersebut dapat dilakukan dengan cara melakukan proses PING.



```

⊟ Frame 1710: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
⊟ Ethernet II, Src: LiteonTe_d4:fe:78 (70:f1:a1:d4:fe:78), Dst: HonHaiPr_27:55:4e (f0:7b:cb:27:55:4e)
⊟ Internet Protocol Version 4, Src: 172.17.33.22 (172.17.33.22), Dst: 172.17.75.250 (172.17.75.250)
⊟ Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x545b [correct]
  Identifier (BE): 256 (0x0100)
  Identifier (LE): 1 (0x0001)
  Sequence number (BE): 1 (0x0001)
  Sequence number (LE): 256 (0x0100)
  [Response To: 1709]
  [Response Time: 161.135 ms]
⊟ Data (32 bytes)
0000  f0 7b cb 27 55 4e 70 f1 a1 d4 fe 78 08 00 45 00  .{.'UNp. ...x..E.
0010  00 3c 28 b2 00 00 80 01 4c dc ac 11 21 16 ac 11  -<(. ... L...l...
0020  4b fa 00 00 54 5b 01 00 00 01 61 62 63 64 65 66  k...T[...]..abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmno pqrstuv
0040  77 61 62 63 64 65 66 67 68 69                    wabcdfgh i

```



Terlihat bahwa pada saat proses aplikasi ping 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, berhasil dilakukan seperti terlihat pada tampilan di atas.

Secara teoritis, *echo request* dan *echo reply* adalah dua tipe pesan yang digunakan untuk melihat apakah tujuan (*destination*) dapat dicapai dan dalam keadaan hidup. Pada saat mengirim ECHO REQUEST, tujuan (*destination*) diharapkan untuk mengirim balik ECHO REPLY yang menandakan tujuan dapat dicapai dan dalam keadaan hidup.

Sesuai dengan tampilan capture dan flow graph, yang bertindak sebagai Source (sumber yang melakukan ping) memiliki IP 172.17.33.22 selalu mengirimkan Echo (ping) request pada proses awal, menuju Destination (tujuan dari ping yang diinginkan sumber)

memiliki IP 172.17.33.22 yang memberikan balasan Echo (ping) reply atau dengan kata lain ping yang dilakukan berhasil sebab sampai ke alamat tujuan.

- b. Tampilan Wireshark saat melakukan monitoring ICMP yang tidak berhasil (destination unreachable), hal tersebut dapat dikarenakan saat melakukan proses PING terjadi error atau suatu proses terputusnya server pada suatu jaringan maka PING gagal.

The screenshot shows the Wireshark interface with a filter set to 'icmp'. The packet list pane displays several ICMP Echo (ping) requests from source 172.17.75.250 to destination 172.16.3.2, and one ICMP Destination unreachable (Port unreachable) response from source 202.155.0.15 to destination 172.17.75.250.

No.	Time	Source	Destination	Protocol	Length	Info
10169	39.0070550	172.17.75.250	172.16.3.2	ICMP	74	Echo (ping) request id=0x0100, seq=45/11520, ttl=128
11549	43.5391100	172.17.75.250	172.16.3.2	ICMP	74	Echo (ping) request id=0x0100, seq=46/11776, ttl=128
12944	48.5322690	172.17.75.250	172.16.3.2	ICMP	74	Echo (ping) request id=0x0100, seq=47/12032, ttl=128
14814	53.5395830	172.17.75.250	172.16.3.2	ICMP	74	Echo (ping) request id=0x0100, seq=48/12288, ttl=128
21162	78.5332030	172.17.75.250	202.155.0.15	ICMP	158	Destination unreachable (Port unreachable)

The packet details pane for frame 14814 shows:

- Frame 14814: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
- Ethernet II, Src: HonHaiPr_27:55:4e (f0:7b:cb:27:55:4e), Dst: Cisco_b6:d3:c0 (00:0b:45:b6:d3:c0)
- Internet Protocol Version 4, Src: 172.17.75.250 (172.17.75.250), Dst: 172.16.3.2 (172.16.3.2)
- Internet Control Message Protocol
 - Type: 8 (Echo (ping) request)
 - Code: 0
 - Checksum: 0x4c2c [correct]
 - Identifier (BE): 256 (0x0100)
 - Identifier (LE): 1 (0x0001)
 - Sequence number (BE): 48 (0x0030)
 - Sequence number (LE): 12288 (0x3000)
- Data (32 bytes)

The packet bytes pane for frame 14814 shows the following hex and ASCII data:

```

0000  00 0b 45 b6 d3 c0 f0 7b cb 27 55 4e 08 00 45 00  ..E....{.'UN..E.
0010  00 3c 25 c3 00 00 80 01 6d e0 ac 11 4b fa ac 10  .<%.... m..K...
0020  03 02 08 00 4c 2c 01 00 00 30 61 62 63 64 65 66  ....L... .0abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69                    wabcdfgh i
  
```

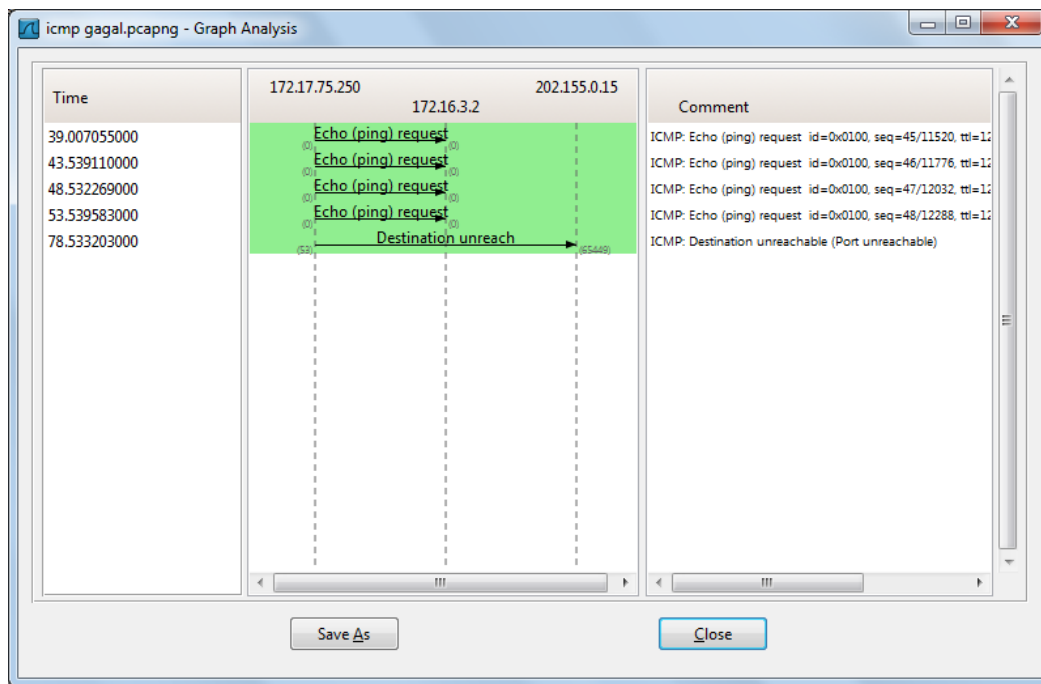
The packet details pane for frame 21162 shows:

- Frame 21162: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits) on interface 0
- Ethernet II, Src: HonHaiPr_27:55:4e (f0:7b:cb:27:55:4e), Dst: Cisco_b6:d3:c0 (00:0b:45:b6:d3:c0)
- Internet Protocol Version 4, Src: 172.17.75.250 (172.17.75.250), Dst: 202.155.0.15 (202.155.0.15)
- Internet Control Message Protocol
 - Type: 3 (Destination unreachable)
 - Code: 3 (Port unreachable)
 - Checksum: 0xc024 [correct]
- Internet Protocol Version 4, Src: 202.155.0.15 (202.155.0.15), Dst: 172.17.75.250 (172.17.75.250)
- User Datagram Protocol, Src Port: domain (53), Dst Port: 65449 (65449)
- Domain Name System (response)

The packet bytes pane for frame 21162 shows the following hex and ASCII data:

```

0000  00 0b 45 b6 d3 c0 f0 7b cb 27 55 4e 08 00 45 00  ..E....{.'UN..E.
0010  00 90 30 58 00 00 80 01 47 5f ac 11 4b fa ca 9b  ..OX.... G...K...
0020  00 0f 03 03 c0 24 00 00 00 00 45 00 00 74 00 00  ....$. .E..T...
0030  40 00 3f 11 78 c3 ca 9b 00 0f ac 11 4b fa 00 35  @.?.x... ..K..5
0040  ff a9 00 60 c9 be 80 ae 81 80 00 01 00 02 00 00  ... ..
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..
  
```



Secara teoritis, Destination unreachable merupakan tipe pesan yang digunakan ketika subnet atau router tidak dapat menemukan tujuan, atau paket dengan DF bit tidak dapat dikirimkan, karena “paket-kecil” jaringan berada pada jalur.

Sesuai dengan tampilan capture dan flow graph, yang bertindak sebagai Source (sumber yang melakukan ping) memiliki IP 172.17.75.250 selalu mengirimkan Echo (ping) request pada proses awal, menuju Destination (tujuan dari ping yang diinginkan sumber) memiliki IP 172.17.3.2, namun belum juga memberikan balasan Echo (ping) reply seperti proses ping yang berhasil malah mendapat balasan Destination unreachable (port unreachable). Dapat diartikan bahwa seperti teori yang ada, bahwa balasan Destination Unreachable, mengindikasikan sebagai laporan bahwa tujuan tidak dapat dijangkau.

Dapat disimpulkan dari analisis menggunakan Wireshark, bahwa pada protokol ICMP memiliki empat jawaban, hal tersebut dapat dilihat lagi pada type dan code di tab Internet protokol, antara lain:

- | | |
|----------------------------|---------------------|
| a. Request | c. Reply |
| Type : 8 | Type : 0 |
| Code : 0 | Code : 0 |
| b. Destination Unreacheble | d. Request Time Out |
| Type : 3 | Type : 0 |
| Code : 3 | Code : 0 |

Biografi Penulis



Annisa Cahyaningtyas. Saat ini sedang menjalani studi D4 di Politeknik Negeri Semarang, Jurusan Teknik Elektro, Program Studi Teknik Telekomunikasi.