

# ICMP (Internet Control Message Protocol)

**Yama Fredian Dwi Saputro**

*fds.yama@gmail.com*

## ***Lisensi Dokumen:***

*Copyright © 2003-2015 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.*

ICMP (Internet Control Message Protocol) adalah protokol yang bertugas mengirimkan pesan-pesan kesalahan dan kondisi lain yang memerlukan perhatian khusus. Pesan / paket ICMP dikirim jika terjadi masalah pada layer IP (layer 3) dan layer atasnya (TCP/UDP) (layer 4). 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.

contoh : hubungan antar router A dan B mengalami masalah, maka router A secara otomatis akan mengirimkan paket ICMP Destination Unreachable ke host pengirim paket yang berusaha melewati host B menuju tujuannya. Dengan adanya pemberitahuan ini maka host tujuan tidak akan terus menerus berusaha mengirimkan paketnya melewati router B.

ICMP (Internet Control Message Protocol) adalah protokol yang bertugas mengirimkan pesan-pesan kesalahan dan kondisi lain yang memerlukan perhatian khusus. Pesan / paket ICMP dikirim jika terjadi masalah pada layer [IP](#) (layer 3) dan layer atasnya (TCP/UDP) (layer 4). 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.

contoh : hubungan antar router A dan B mengalami masalah, maka router A secara otomatis akan mengirimkan paket ICMP Destination Unreachable ke host pengirim paket yang berusaha melewati host B menuju tujuannya. Dengan adanya pemberitahuan ini maka host tujuan tidak akan terus menerus berusaha mengirimkan paketnya melewati router B.

Ada dua tipe pesan yang dapat dihasilkan ICMP :

1. **ICMP Error Message** (dihasilkan jika terjadi kesalahan [jaringan](#))
2. **ICMP Query Message** (dihasilkan jika pengirim paket mengirimkan informasi tertentu yang berkaitan dengan kondisi [jaringan](#)).

1. **ICMP Error Message** dibagi menjadi beberapa jenis :
  - a. **Destination Unreachable**, dihasilkan oleh router jika pengirim paket mengalami kegagalan akibat masalah putusnya jalur baik secara fisik maupun logic.
    - Destination Unreacheable dibagi lagi menjadi beberapa jenis :
      - Network Unreacheable, jika [jaringan](#) tujuan tak dapat dihubungi.
      - Host Unreacheable, jika host tujuan tak bisa dihubungi.
      - Protocol At Destination is Unreacheable, jika di tujuan tak tersedia protokol tersebut.
      - Destination Host is Unknown, jika host tujuan tidak diketahui.
      - Destination Network is Unknown, jika network tujuan tidak diketahui.
  - b. **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.
  - c. **Parameter Problem**, paket ini dikirim jika terdapat kesalahan parameter pada header paket [IP](#).
  - d. **Source Quench**, Paket ICMP ini dikirimkan jika router tujuan mengalami kongesti. Sebagai respons atas paket ini pihak pengirim paket harus memperlambat pengiriman paketnya.
  - e. **Redirect**, paket ini dikirimkan jika router merasa host mengirimkan paket [IP](#) melalui router yang salah. Paket ini seharusnya dikirimkan melalui router lain.
2. **ICMP Query Message** Terdiri atas :
  - **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.
  - **Timestamp dan Timestamp Reply**, Menghasilkan informasi waktu yang diperlukan sistem tujuan untuk memproses suatu paket.
  - **Address mask**, untuk mengetahui beberapa netmask yang harus digunakan suatu host dalam suatu network.

Pesan iCMP memiliki format khusus. Masing-masing tipe pesan ICMP ditunjukkan oleh gambar. Semua format pesan ICMP dimulai dengan tiga field yang sama:

- Type
- Code
- Checksum

ICMP Message type	
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

<b>14</b>	<b>Timestamp Reply</b>
<b>15</b>	<b>Information Request</b>
<b>16</b>	<b>Information Reply</b>
<b>17</b>	<b>Address Mask Request</b>
<b>18</b>	<b>Address Moks Reply</b>

Field tipe menunjukkan tipe dari pesan ICMP yang dikirim. Field code menunjukkan informasi yang khusus untuk tipe pesan. Checksum field sebagai tipe lain dari paket yang digunakan untuk mem-verifikasi integritas data. Berikut adalah pesan echo request dan echo reply ICMP

<b>0</b>	<b>8</b>	<b>16</b>	<b>31</b>
<b>Type (0 or 8)</b>	<b>Code (0)</b>	<b>Cheksum</b>	
<b>Identifier</b>		<b>Sequence number</b>	
<b>Operational Data</b>			

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.

#### **Pesan Destination Unreachable**

Datagram tidak selalu dapat di-forward ke tujuannya. Masalah di hardware, konfigurasi protokol yang salah, interface mati dan informasi routing yang salah adalah factor-faktor penyebabnya. Dalam hal ini, ICMP mengirimkan pesan ke pengirim pesan destination unreachable dimana datagram tidak dapat di-forward ke tujuan.

Pesan destination unreachable

<b>0</b>	<b>8</b>	<b>16</b>	<b>31</b>
<b>Type (3)</b>	<b>Code (0)</b>	<b>Cheksum</b>	
<b>Unused (must be zero)</b>			
<b>Internet Header + First 64 Bits of datagram</b>			

Gambar di atas menunjukkan header pesan destination unreachable. Nilai 3 dari field tipe menunjukkan pesan destination unreachable. Nilai kode menunjukkan alasan paket dapat dikirim. Nilai kode 0 berarti jaringan unreachable.

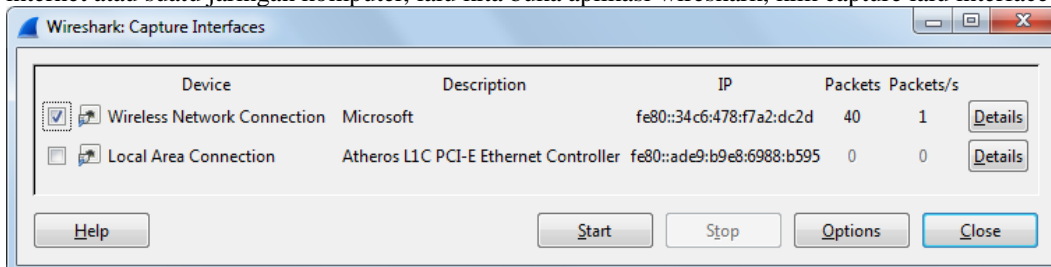
**Nilai kode untuk pesan destination unreachable**

<b>0</b>	<b>Net unreachable</b>
<b>1</b>	<b>Host unreachable</b>
<b>2</b>	<b>Protocol unreachable</b>
<b>3</b>	<b>Port unreachable</b>
<b>4</b>	<b>Fragmentation needed and DF ste</b>
<b>5</b>	<b>Source route failed</b>
<b>6</b>	<b>Destination network unknown</b>
<b>7</b>	<b>Destination host unknown</b>
<b>8</b>	<b>Source host isolated</b>
<b>9</b>	<b>Communcation with destination network administratively prohibited</b>
<b>10</b>	<b>Communcation with destination host administratively prohibited</b>
<b>11</b>	<b>Network unreachable for type of service</b>
<b>12</b>	<b>Host unreachable for type of service</b>

Pesan destination unreachable juga mungkin dikirim ketika fragmentasi paket dibutuhkan untuk mem-forward paket. Fragmentasi selalu dibutuhkan saat datagram di-forward dari jaringan token ring ke jaringan Ethernet. Jika datagram tidak mengijinkan fragmentasi datagram, maka paket tidak dapat di-forward sehingga pesan destination unreachable dikirim. Pesan destination unreachable juga dibangkitkan jika layanan IP seperti FTP atau Web tidak ada.

❖ **ICMP pada wireshark**

Kita dapat memonitoring ICMP menggunakan software wireshark, pertama kita sudah terhubung dengan internet atau suatu jaringan komputer, lalu kita buka aplikasi wireshark, klik capture lalu interface



Setelah kita pilih device nya kita klik start, untuk melihat protocol ICMP nya kita melakukan PING terlebih dahulu di command prompt.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\DELL>ping google.com

Pinging google.com [74.125.68.138] with 32 bytes of data:
Reply from 74.125.68.138: bytes=32 time=61ms TTL=45
Reply from 74.125.68.138: bytes=32 time=53ms TTL=45
Reply from 74.125.68.138: bytes=32 time=49ms TTL=45
Reply from 74.125.68.138: bytes=32 time=59ms TTL=45

Ping statistics for 74.125.68.138:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 49ms, Maximum = 61ms, Average = 55ms

C:\Users\DELL>_
```

Lalu untuk melihat protocol ICMP saja kita bisa memfilter protocol yang muncul dengan mengetikkan icmp di kolom filter

The screenshot shows the Wireshark interface with the filter 'icmp' applied. The packet list pane displays a series of ICMP Echo (ping) requests and replies. The packet details pane shows the structure of an ICMP Echo (ping) request, including fields like Type, Code, Checksum, Identifier, Sequence number, and Data.

No.	Time	Source	Destination	Protocol	Length	Info
85	9.26223800	10.10.32.73	173.194.126.98	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 86)
86	9.32834900	173.194.126.98	10.10.32.73	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=52 (request in 85)
94	10.01030900	10.10.32.73	173.194.126.98	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 93)
95	10.35505300	173.194.126.98	10.10.32.73	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=52 (request in 94)
99	11.27710500	10.10.32.73	173.194.126.98	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 100)
100	11.39916000	173.194.126.98	10.10.32.73	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=52 (request in 99)
104	12.27909600	10.10.32.73	173.194.126.98	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 105)
105	12.35728300	173.194.126.98	10.10.32.73	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=52 (request in 104)
183	19.41149000	10.10.32.73	98.138.253.109	ICMP	74	Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 192)
192	19.80543300	98.138.253.109	10.10.32.73	ICMP	74	Echo (ping) reply id=0x0001, seq=9/2304, ttl=48 (request in 183)
198	20.41244300	10.10.32.73	98.138.253.109	ICMP	74	Echo (ping) request id=0x0001, seq=10/2560, ttl=128 (reply in 205)
205	20.74469600	98.138.253.109	10.10.32.73	ICMP	74	Echo (ping) reply id=0x0001, seq=10/2560, ttl=48 (request in 198)
209	21.41446700	10.10.32.73	98.138.253.109	ICMP	74	Echo (ping) request id=0x0001, seq=11/2816, ttl=128 (reply in 211)
211	21.79812000	98.138.253.109	10.10.32.73	ICMP	74	Echo (ping) reply id=0x0001, seq=11/2816, ttl=48 (request in 209)
217	22.41647900	10.10.32.73	98.138.253.109	ICMP	74	Echo (ping) request id=0x0001, seq=12/3072, ttl=128 (reply in 220)
220	22.84422600	98.138.253.109	10.10.32.73	ICMP	74	Echo (ping) reply id=0x0001, seq=12/3072, ttl=48 (request in 217)

Gambar di atas merupakan hasil dari PING ke google yang di lakukan di cmd

```

217 22.4164790 10.10.32.73 98.138.253.109 ICMP 74 Echo (ping) request id=0x0001, seq=
<
Ethernet II, Src: JuniperN_c3:de:40 (f8:c0:01:c3:de:40), Dst: QuantaMi_76:64:c1 (20:7c:8f:76:64:c1)
Internet Protocol Version 4, Src: 10.10.32.73 (10.10.32.73), Dst: 173.194.126.98 (173.194.126.98)
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x4d55 [correct]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence number (BE): 6 (0x0006)
  Sequence number (LE): 1536 (0x0600)
  [Response frame: 95]
  Data (32 bytes)
    Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
    [Length: 32]
0000 f8 c0 01 c3 de 40 20 7c 8f 76 64 c1 08 00 45 00 |....@|.vd...E.
0010 00 3c 2d 09 00 00 80 01 b7 40 0a 0a 20 49 ad c2 |.<...4./...-b..
0020 7e 62 08 00 4d 55 00 01 00 06 61 62 63 64 65 66 |I..uu...abcdef
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 |wabcdefg hi
    
```

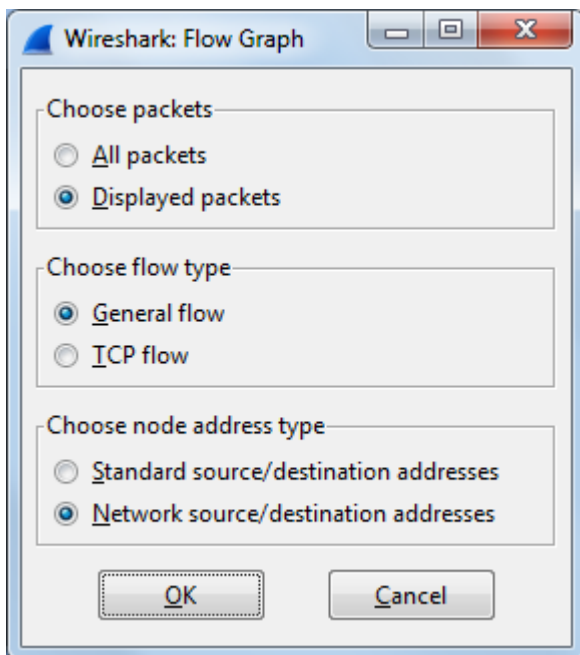
Gambar di atas dapat di jelaskan type pesan dari ICMP di atas adalah 8. Pada tabel type pesan di atas di jelaskan bahwa no 8 adalah *echo request*, yaitu type pesan ketika kita meminta untuk menghubungkan ke google.com.

```

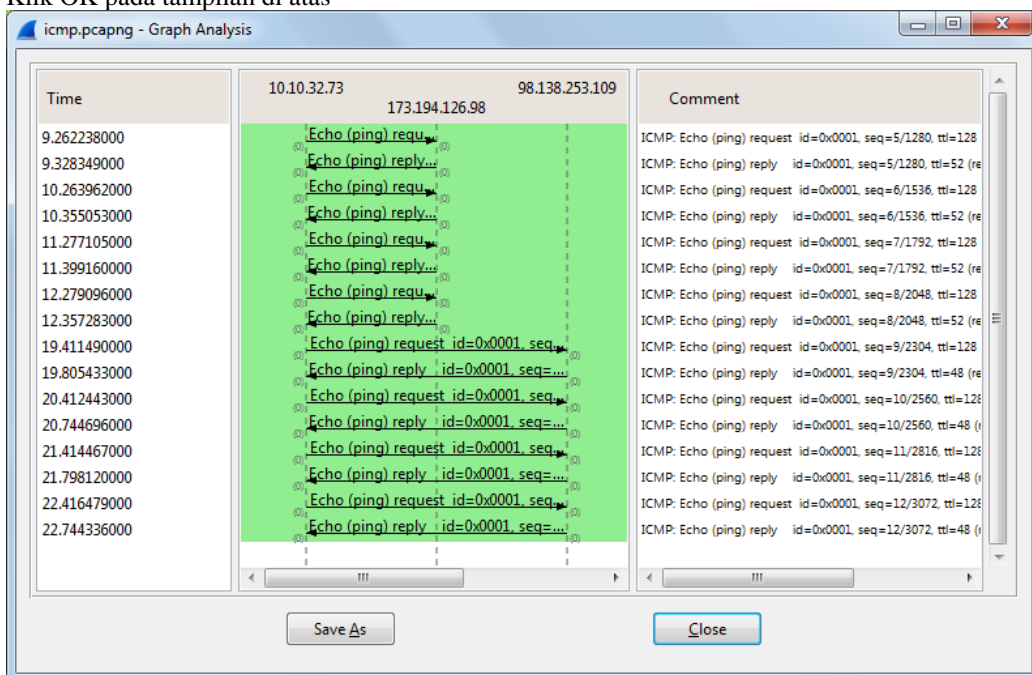
Frame 95: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: JuniperN_c3:de:40 (f8:c0:01:c3:de:40), Dst: QuantaMi_76:64:c1 (20:7c:8f:76:64:c1)
Internet Protocol Version 4, Src: 173.194.126.98 (173.194.126.98), Dst: 10.10.32.73 (10.10.32.73)
Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x5555 [correct]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence number (BE): 6 (0x0006)
  Sequence number (LE): 1536 (0x0600)
  [Request frame: 94]
  [Response time: 91,091 ms]
  Data (32 bytes)
0000 20 7c 8f 76 64 c1 f8 c0 01 c3 de 40 08 00 45 00 |.vd... ..@..E.
0010 00 3c 00 c7 00 00 34 01 2f 83 ad c2 7e 62 0a 0a |.<...4./...-b..
0020 20 49 00 00 55 55 00 01 00 06 61 62 63 64 65 66 |I..uu...abcdef
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 |wabcdefg hi
    
```

Sedangkan gambar di atas bisa di jelaskan type pesannya adalah 0. Itu berarti adalah echo reply. Yang di maksud echo reply berarti kita menjawab dari request PING tadi sehingga kita bisa menghubungkan ke google.com.

Jika kita ini melihat flow graph nya kita bisa klik pada statistic lalu flow graph



Klik OK pada tampilan di atas



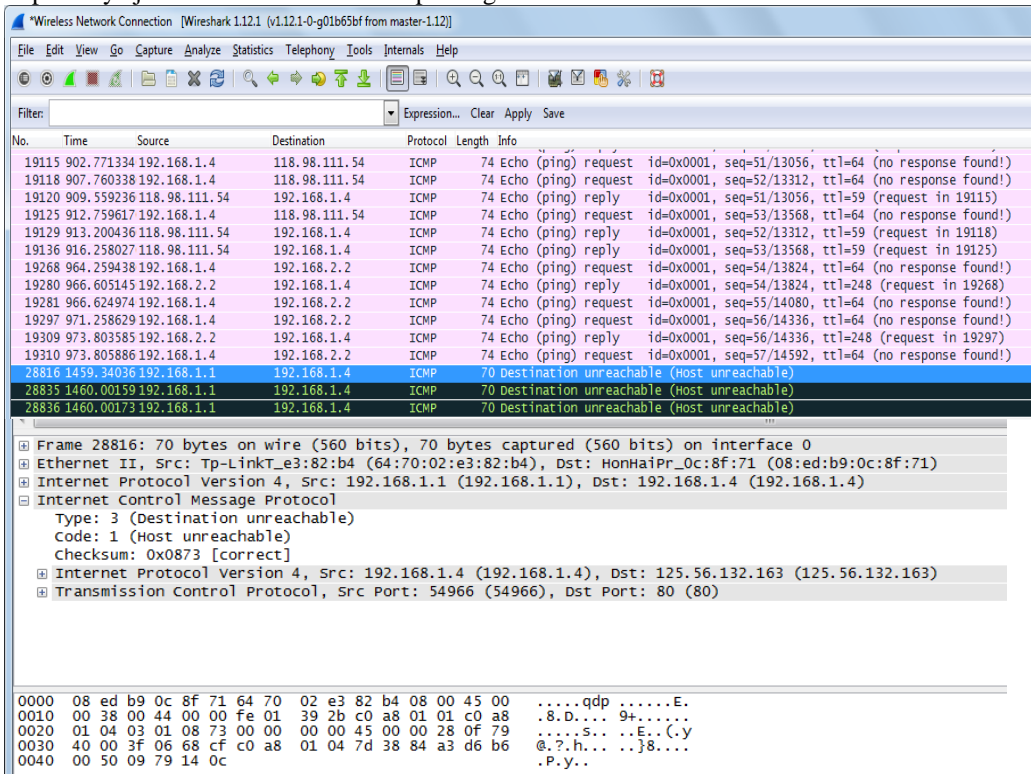
*echo request* dan *echo reply* adalah dua tipe pesan yang digunakan untuk melihat apakah tujuan (*destination*) dapat dicapai .Pada saat mengirim ECHO REQUEST, tujuan (*destination*) diharapkan untuk mengirim balik ECHO REPLY yang menandakan tujuan dapat dicapai.

Sesuai dengan tampilan capture dan flow graph, yang bertindak sebagai Source (sumber yang melakukan ping) memiliki IP 173.194.126.98 selalu mengirimkan Echo (ping) request pada proses awal, menuju Destination (tujuan dari ping yang diinginkan sumber) yang memiliki IP 173.194.126.98 yang memberikan balasan Echo (ping) reply atau dengan kata lain ping yang dilakukan berhasil sebab sampai ke alamat tujuan.

Lalu ketika paket tidak dapat di terima atau biasanya di sebut destination Unreachable. Hal ini terjadi karena pengiriman paket mengalami kegagalan karena terjadi error atau

Komunitas eLearning IlmuKomputer.Com  
Copyright © 2003-2014 IlmuKomputer.Com

terputusnya jalur baik secara fisik maupun logic.



Gambar di atas dapat dijelaskan bahwa 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. Ada keterangan di atas type pesan yang tertera adalah 3, yang dalam tael type pesan itu meruapakan destination unreaceble, yaitu bahwa proses PING tidak berjalan dengan baik, dan IP destinationnya tidak dapat di jangkau

## Biografi Penulis

Yama Fresdian Dwi Saputro. Menyelesaikan Program D4 Telekomunikasi di Politeknik Negeri Semarang.