

il protocollo ICMP e i comandi ping e traceroute

g. di battista, m. patrignani, m. pizzonia

130-icmp-05 copyright ©2020 g. di battista, m. patrignani, m. pizzonia

1

nota di copyright

- questo insieme di slides è protetto dalle leggi sul copyright
- il titolo ed il copyright relativi alle slides (inclusi, ma non limitatamente, immagini, foto, animazioni, video, audio, musica e testo) sono di proprietà degli autori indicati sulla prima pagina
- le slides possono essere riprodotte ed utilizzate liberamente, non a fini di lucro, da università e scuole pubbliche e da istituti pubblici di ricerca
- ogni altro uso o riproduzione è vietata, se non esplicitamente autorizzata per iscritto, a priori, da parte degli autori
- l'informazione contenuta in queste slides è fornita per scopi didattici e non può essere usata in progetti di reti, impianti, prodotti, ecc.
- gli autori non si assumono nessuna responsabilità per il contenuto delle slides, che sono comunque soggette a cambiamento
- questa nota di copyright non deve essere mai rimossa e deve essere riportata anche in casi di uso parziale

130-icmp-05 copyright ©2020 g. di battista, m. patrignani, m. pizzonia

2

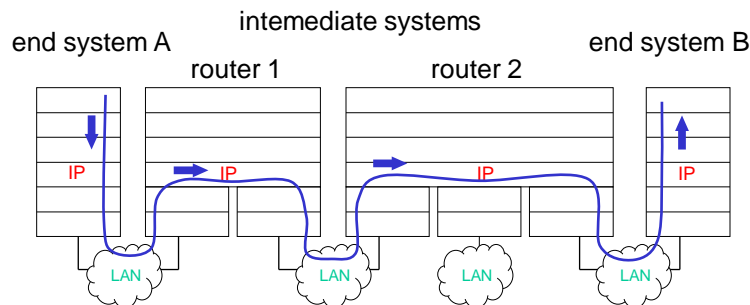
il protocollo IP e l'approccio best effort

- il protocollo IP ha un approccio *best effort* (letteralmente: sforzo migliore): non è in grado di garantire la consegna dei pacchetti, ma esegue dei tentativi, al meglio delle possibilità di cui dispone
- alcuni pacchetti possono essere scartati da IP: sono “*dropped on the floor*”, cioè “lasciati cadere in terra”
 - i livelli superiori provvederanno alle eventuali ritrasmissioni
- un semplice servizio di *error-reporting* è offerto da ICMP (*Internet Control Message Protocol*, cioè “protocollo per i messaggi di controllo in internet”)
- ICMP offre anche dei messaggi che consentono di richiedere ed ottenere informazioni

130-icmp-05 copyright ©2020 g. di battista, m. patrignani, m. pizzonia

3

richiami terminologici



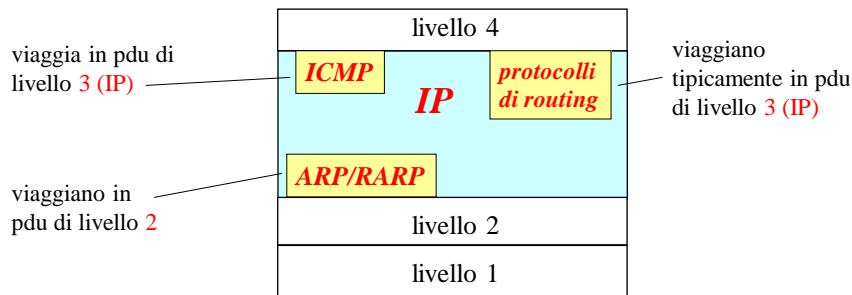
- **hop**: (“salto” oppure “scalo”), un computer intermedio tra la sorgente e la destinazione del pacchetto
- **tempo di vita**: (ttl, cioè “time to live”) misura del tempo residuo di validità del pacchetto
 - conta gli hop rimanenti
 - ogni router decrementa il ttl di 1
 - i pacchetti con ttl=0 vengono scartati

130-icmp-05 copyright ©2020 g. di battista, m. patrignani, m. pizzonia

4

protocolli di supporto del livello 3

- portano informazioni *di controllo* e non offrono direttamente servizi
- esempi:



130-icmp-05 copyright ©2020 g. di battista, m. patrignani, m. pizzonia

5

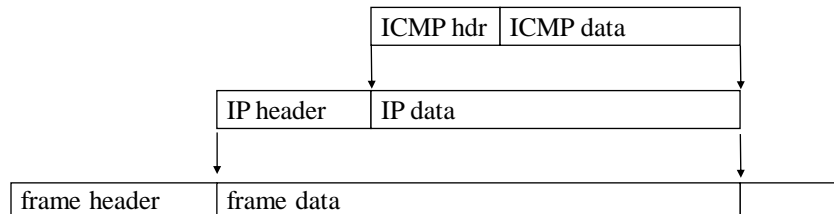
il protocollo ICMP - regole

- la prima specifica del protocollo è contenuta nella RFC 792
- regola 1: nessun messaggio ICMP viene generato a seguito di eventuali errori rilevati su altri messaggi ICMP
- regola 2: se il pacchetto viene frammentato solo il primo frammento può generare messaggi di errore ICMP
- regola 3: i broadcast e multicast non generano ICMP

130-icmp-05 copyright ©2020 g. di battista, m. patrignani, m. pizzonia

6

il protocollo ICMP - imbustamento



130-icmp-05 copyright ©2020 g. di battista, m. patrignani, m. pizzonia

7

messaggi di *destination unreachable*

sono causati da un pacchetto scartato e possono essere di vari tipi; i principali sono:

- **network unreachable**: un gateway vede la rete destinazione a distanza infinita
- **host unreachable**: l'host destinazione non risponde ad una chiamata ARP
- **protocol unreachable**: l'host destinazione non conosce il protocollo nel pacchetto
- **port unreachable**: la *port* specificata non è raggiungibile
- **fragmentation needed and DF set**: il pacchetto non può essere frammentato

130-icmp-05 copyright ©2020 g. di battista, m. patrignani, m. pizzonia

8

messaggi di *tempo scaduto*

sono causati da un pacchetto scartato perché è stato superato il massimo tempo ammissibile per la consegna:

- **TIME_EXCEEDED** (tempo scaduto)
 - il pacchetto ha TTL=0 e quindi viene scartato

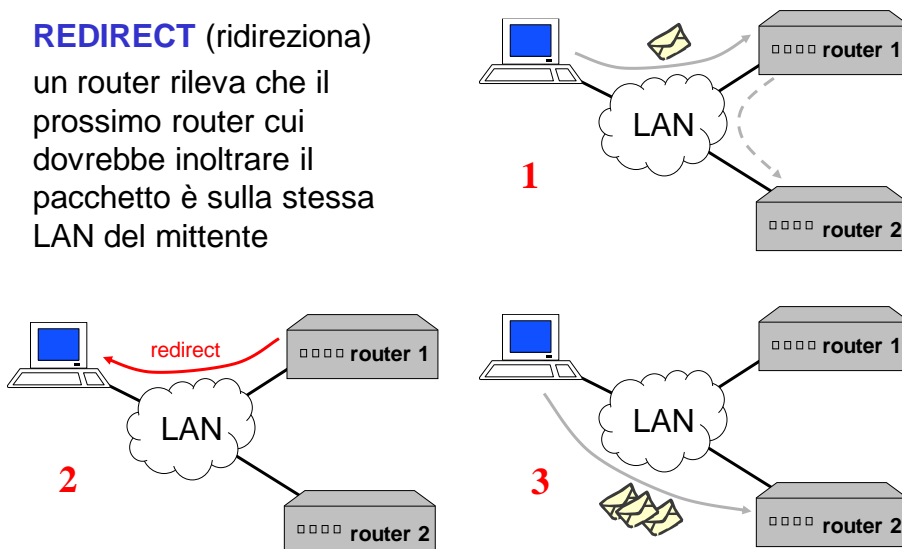
130-icmp-05 copyright ©2020 g. di battista, m. patrignani, m. pizzonia

9

messaggi di *redirection*

REDIRECT (ridireziona)

un router rileva che il prossimo router cui dovrebbe inoltrare il pacchetto è sulla stessa LAN del mittente



130-icmp-05 copyright ©2020 g. di battista, m. patrignani, m. pizzonia

10

messaggi di eco

- **ECHO_REQUEST e REPLY** (richiesta di eco e relativa risposta)
 - controllo di raggiungibilità di un host
- **TIMESTAMP e TIMESTAMP_REPLY** come **ECHO**, più informazioni su orario invio
 - misura di velocità del collegamento
 - sincronizzazione (approssimativa) dell'ora di sistema

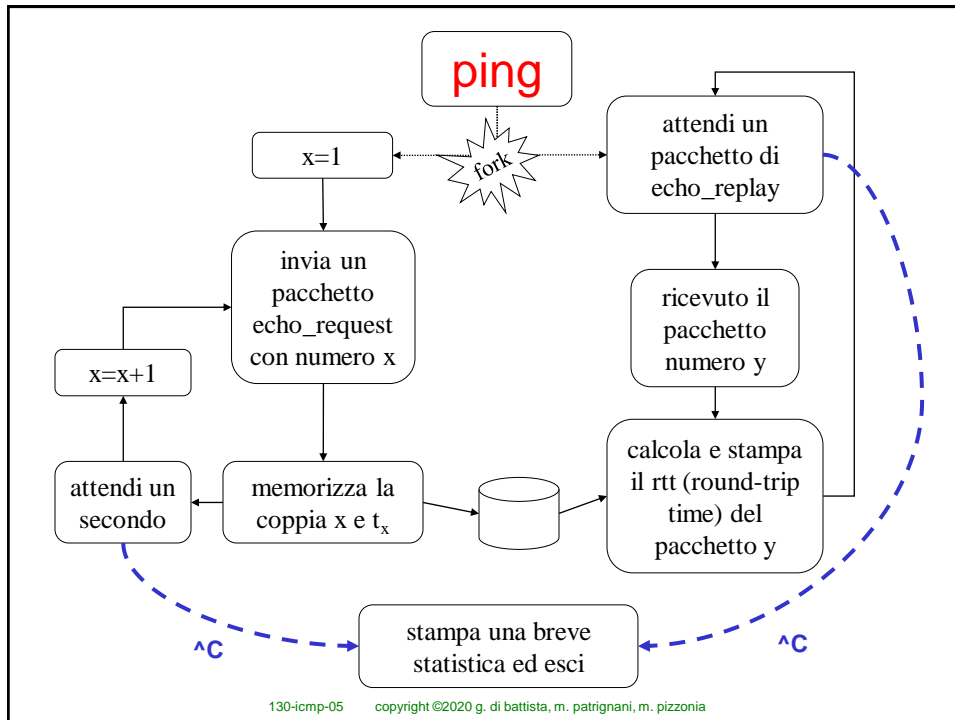
130-icmp-05 copyright ©2020 g. di battista, m. patrignani, m. pizzonia

11

il comando ping

130-icmp-05 copyright ©2020 g. di battista, m. patrignani, m. pizzonia

12



13

un esempio di ping...

giga:~> **ping wilma.cs.brown.edu**

PING qua.cs.brown.edu (128.148.32.110) 56(84) bytes of data.

64 bytes from qua.cs.brown.edu (128.148.32.110): icmp_seq=1 ttl=241 time=137 ms

64 bytes from qua.cs.brown.edu (128.148.32.110): icmp_seq=2 ttl=241 time=136 ms

64 bytes from qua.cs.brown.edu (128.148.32.110): icmp_seq=3 ttl=241 time=143 ms

64 bytes from qua.cs.brown.edu (128.148.32.110): icmp_seq=4 ttl=241 time=137 ms

64 bytes from qua.cs.brown.edu (128.148.32.110): icmp_seq=5 ttl=241 time=138 ms

64 bytes from qua.cs.brown.edu (128.148.32.110): icmp_seq=6 ttl=241 time=139 ms

^C

--- qua.cs.brown.edu ping statistics ---

6 packets transmitted, 6 received, 0% packet loss, time 5058ms

rtt min/avg/max/mdev = 136.446/138.911/143.975/2.543 ms

giga:~>

130-icmp-05 copyright ©2020 g. di battista, m. patrignani, m. pizzonia

14

...e i relativi pacchetti

```
giga:~# tcpdump -n 'icmp'
tcpdump: listening on eth0
19:58:07.785101 193.204.161.49 > 128.148.32.110: icmp: echo request (DF)
19:58:07.922516 128.148.32.110 > 193.204.161.49: icmp: echo reply
19:58:08.803773 193.204.161.49 > 128.148.32.110: icmp: echo request (DF)
19:58:08.940206 128.148.32.110 > 193.204.161.49: icmp: echo reply
19:58:09.813816 193.204.161.49 > 128.148.32.110: icmp: echo request (DF)
19:58:09.957780 128.148.32.110 > 193.204.161.49: icmp: echo reply
19:58:10.823850 193.204.161.49 > 128.148.32.110: icmp: echo request (DF)
19:58:10.960933 128.148.32.110 > 193.204.161.49: icmp: echo reply
19:58:11.834549 193.204.161.49 > 128.148.32.110: icmp: echo request (DF)
19:58:11.973295 128.148.32.110 > 193.204.161.49: icmp: echo reply
19:58:12.843931 193.204.161.49 > 128.148.32.110: icmp: echo request (DF)
19:58:12.983688 128.148.32.110 > 193.204.161.49: icmp: echo reply
^C
13 packets received by filter
0 packets dropped by kernel
giga:~#
```

130-icmp-05 copyright ©2020 g. di battista, m. patrignani, m. pizzonia

15

ping su indirizzo broadcast

```
<patrigna@pascal ~->ping 193.204.162.255
PING 193.204.162.255: (193.204.162.255): 56 data bytes
64 bytes from 193.204.162.32: icmp_seq=0 ttl=255 time=0 ms
64 bytes from 193.204.162.7: icmp_seq=0 ttl=255 time=1 ms (DUP!)
64 bytes from 193.204.162.9: icmp_seq=0 ttl=255 time=5 ms (DUP!)
64 bytes from 193.204.162.113: icmp_seq=0 ttl=255 time=6 ms (DUP!)
64 bytes from 193.204.162.114: icmp_seq=0 ttl=255 time=7 ms (DUP!)
64 bytes from 193.204.162.20: icmp_seq=0 ttl=255 time=8 ms (DUP!)
64 bytes from 193.204.162.196: icmp_seq=0 ttl=60 time=9 ms (DUP!)
64 bytes from 193.204.162.152: icmp_seq=0 ttl=255 time=10 ms (DUP!)
64 bytes from 193.204.162.215: icmp_seq=0 ttl=64 time=10 ms (DUP!)
64 bytes from 193.204.162.189: icmp_seq=0 ttl=64 time=11 ms (DUP!)
64 bytes from 193.204.162.131: icmp_seq=0 ttl=255 time=11 ms (DUP!)
64 bytes from 193.204.162.128: icmp_seq=0 ttl=64 time=11 ms (DUP!)
64 bytes from 193.204.162.22: icmp_seq=0 ttl=60 time=12 ms (DUP!)
64 bytes from 193.204.162.108: icmp_seq=0 ttl=64 time=12 ms (DUP!)
64 bytes from 193.204.162.194: icmp_seq=0 ttl=63 time=13 ms (DUP!)
....
```

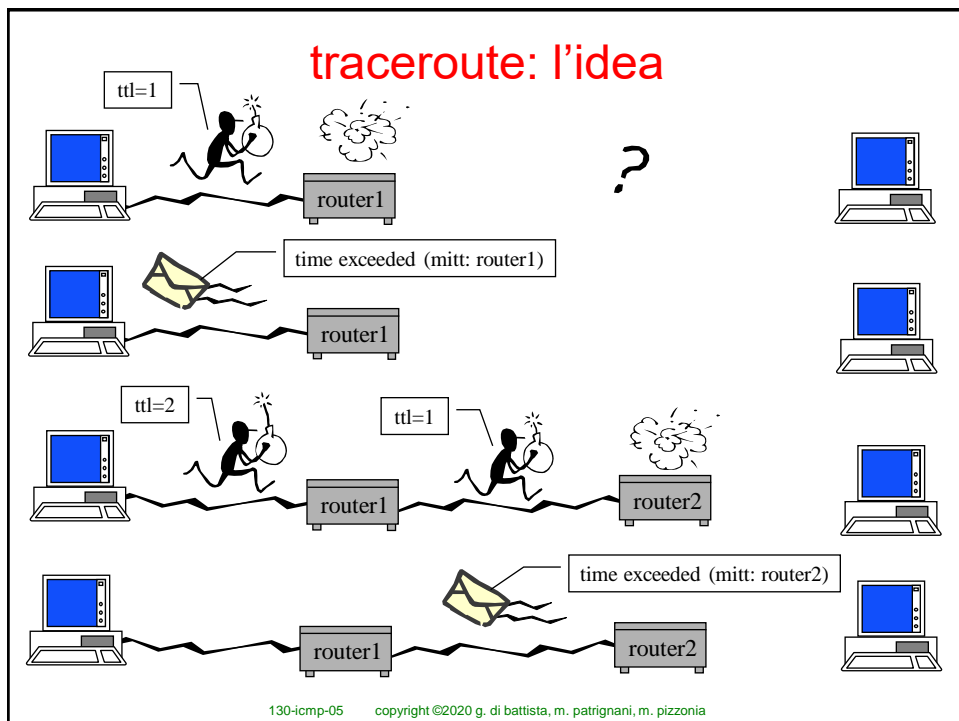
130-icmp-05 copyright ©2020 g. di battista, m. patrignani, m. pizzonia

16

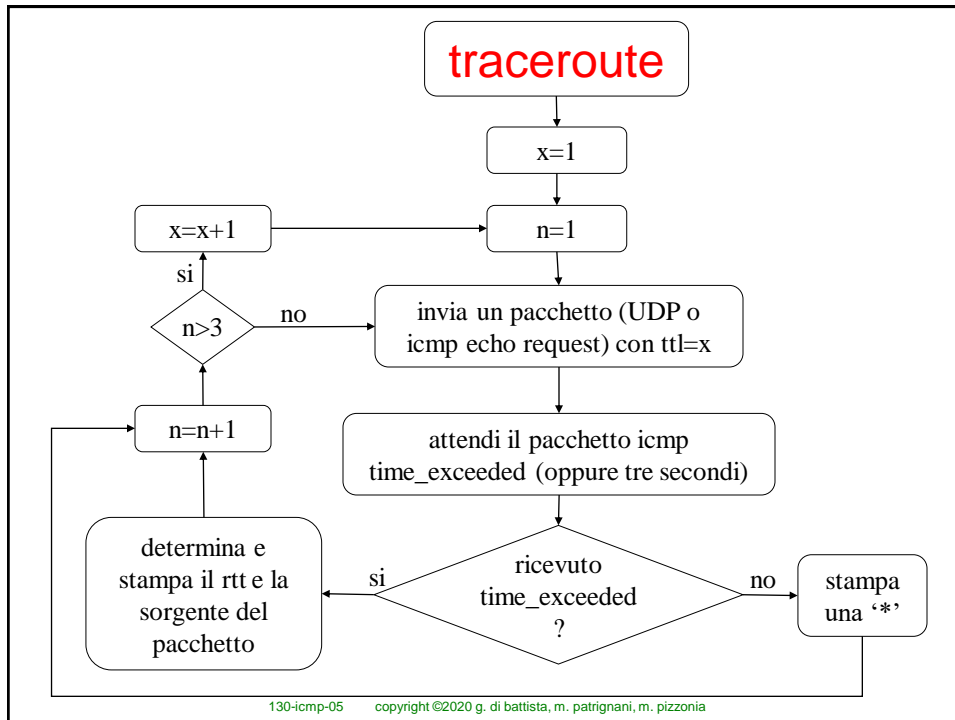
il comando traceroute (tracert per windows)

130-icmp-05 copyright ©2020 g. di battista, m. patrignani, m. pizzonia

17



18



19

un esempio di tracert

PS C:\Users\Pino> tracert 128.148.32.12

Traccia instradamento verso 128.148.32.12
su un massimo di 30 punti di passaggio:

```

1  3 ms  4 ms  3 ms modemtim.homenet.telecomitalia.it [192.168.1.1]
2  * ms  * ms  * ms Richiesta scaduta.
3  10 ms 26 ms 15 ms 172.17.48.50
4  8 ms  8 ms  7 ms 172.17.54.156
5  18 ms 10 ms 10 ms 172.19.177.36
6  21 ms 19 ms 19 ms 172.19.177.2
7  18 ms 16 ms 15 ms etrun49.milano50.mil.seabone.net [195.22.205.116]
8  20 ms 19 ms 19 ms ae20.milano51.mil.seabone.net [195.22.205.13]
9  17 ms 15 ms 16 ms ae8.cr1-mil2.ip4.gtt.net [46.33.83.178]
10 244 ms 199 ms 199 ms ae1.cr8-nyc2.ip4.gtt.net [89.149.128.166]
11 130 ms 203 ms 203 ms ip4.gtt.net [208.116.133.154]
12 117 ms 201 ms 119 ms osn-springfieldlight.oshean.org [198.7.224.114]
13 129 ms 160 ms 202 ms 131.109.200.6
14  * ms  * ms  * ms Richiesta scaduta.
15  * ms  * ms  * ms Richiesta scaduta.
16  * ms  * ms  * ms Richiesta scaduta.
17 127 ms 125 ms 239 ms www.cs.brown.edu [128.148.32.12]
  
```

Traccia completata.

130-icmp-05 copyright ©2020 g. di battista, m. patrignani, m. pizzonia

20

un esempio di traceroute

```
<utente@pascal ~->traceroute wilma.cs.brown.edu
traceroute to wilma.cs.brown.edu (128.148.19.15), 30 hops max, 40 byte packets
 1 gw1.fis.uniroma3.it (193.204.160.1) 3 ms 3 ms 2 ms
 2 141.108.132.1 (141.108.132.1) 832 ms 967 ms 402 ms
 3 mp4rm1.roma1.infn.it (141.108.127.6) 267 ms 106 ms 417 ms
 4 atm-garrten-rm.infn.it (192.135.31.5) 100 ms 939 ms 839 ms
 5 cnafint-ten34.infn.it (192.135.34.21) 1100 ms * 1056 ms
 6 mix-serial3-4.Washington.mci.net (204.189.152.161) 618 ms * *
 7 * core1-fddi-0.Washington.mci.net (204.70.2.1) 1249 ms *
 8 * * *
 9 wtn-bbn-nap.Washington.mci.net (206.157.77.218) 766 ms * *
10 * * chicago1-br1.bbnplanet.net (4.0.1.5) 857 ms
11 * * *
12 * boston1-br1.bbnplanet.net (4.0.2.245) 846 ms *
13 boston1-br2.bbnplanet.net (4.0.2.250) 680 ms * *
14 * * boston1-mr4.bbnplanet.net (4.0.44.19) 648 ms
15 providence-cr1.bbnplanet.net (4.0.45.106) 416 ms providence-
   cr1.bbnplanet.net (4.0.45.102) 1298 ms *
16 brown.bbnplanet.net (131.192.32.2) 1444 ms 615 ms 802 ms
17 * * *
18 * ftp.cs.brown.edu (128.148.19.15) 834 ms 435 ms
<utente@pascal ~->
```

130-icmp-05 copyright ©2020 g. di battista, m. patrignani, m. pizzonia

21

un altro esempio di traceroute...

```
giga:~> traceroute www.caspur.it
traceroute to srv.caspur.it (193.204.5.26), 30 hops max, 40 byte
packets
 1 172.16.119.1 (172.16.119.1) 1 ms 1 ms 1 ms
 2 172.16.50.1 (172.16.50.1) 14 ms 21 ms 12 ms
 3 rc-uniroma3.rm.garr.net (193.206.131.145) 17 ms 15 ms 15
   ms
 4 rt-rc-1.rm.garr.net (193.206.134.161) 16 ms 17 ms 15 ms
 5 rtg-rt-2.rm.garr.net (193.206.134.230) 18 ms 16 ms 18 ms
 6 caspur-rc.rm.garr.net (193.206.131.54) 72 ms 21 ms 20 ms
 7 srv.caspur.it (193.204.5.26) 61 ms 78 ms 17 ms
giga:~>
```

130-icmp-05 copyright ©2020 g. di battista, m. patrignani, m. pizzonia

22

...e i relativi pacchetti (1)

```
giga:~# tcpdump -nv 'icmp or udp'
tcpdump: listening on eth0
13:00:28.216039 193.204.161.49 > 193.204.5.26: udp 12 [ttl 1] (len 40)
13:00:28.216919 172.16.119.1 > 193.204.161.49: icmp: time exceeded in-transit (ttl 255, len 56)
13:00:28.218197 193.204.161.49 > 193.204.5.26: udp 12 [ttl 1] (len 40)
13:00:28.219032 172.16.119.1 > 193.204.161.49: icmp: time exceeded in-transit (ttl 255, len 56)
13:00:28.219154 193.204.161.49 > 193.204.5.26: udp 12 [ttl 1] (len 40)
13:00:28.220043 172.16.119.1 > 193.204.161.49: icmp: time exceeded in-transit (ttl 255, len 56)
13:00:28.220152 193.204.161.49 > 193.204.5.26: udp 12 (ttl 2, len 40)
13:00:28.233651 172.16.50.1 > 193.204.161.49: icmp: time exceeded in-transit (ttl 254, len 56)
13:00:28.234865 193.204.161.49 > 193.204.5.26: udp 12 (ttl 2, len 40)
13:00:28.255356 172.16.50.1 > 193.204.161.49: icmp: time exceeded in-transit (ttl 254, len 56)
13:00:28.255460 193.204.161.49 > 193.204.5.26: udp 12 (ttl 2, len 40)
13:00:28.266927 172.16.50.1 > 193.204.161.49: icmp: time exceeded in-transit (ttl 254, len 56)
13:00:28.267047 193.204.161.49 > 193.204.5.26: udp 12 (ttl 3, len 40)
13:00:28.283795 193.206.131.145 > 193.204.161.49: icmp: time exceeded in-transit (ttl 253, len 56)
13:00:28.285814 193.204.161.49 > 193.204.5.26: udp 12 (ttl 3, len 40)
13:00:28.300339 193.206.131.145 > 193.204.161.49: icmp: time exceeded in-transit (ttl 253, len 56)
13:00:28.300437 193.204.161.49 > 193.204.5.26: udp 12 (ttl 3, len 40)
13:00:28.315662 193.206.131.145 > 193.204.161.49: icmp: time exceeded in-transit (ttl 253, len 56)
13:00:28.315785 193.204.161.49 > 193.204.5.26: udp 12 (ttl 4, len 40)
13:00:28.331840 193.206.134.161 > 193.204.161.49: icmp: time exceeded in-transit (ttl 252, len 56)
13:00:28.333629 193.204.161.49 > 193.204.5.26: udp 12 (ttl 4, len 40)
13:00:28.350656 193.206.134.161 > 193.204.161.49: icmp: time exceeded in-transit (ttl 252, len 56)
13:00:28.350757 193.204.161.49 > 193.204.5.26: udp 12 (ttl 4, len 40)
13:00:28.365486 193.206.134.161 > 193.204.161.49: icmp: time exceeded in-transit (ttl 252, len 56)
...
130-icmp-05 copyright ©2020 g. di battista, m. patrignani, m. pizzonia
```

23

...e i relativi pacchetti (2)

```
...
13:00:28.365616 193.204.161.49 > 193.204.5.26: udp 12 (ttl 5, len 40)
13:00:28.383752 193.206.134.230 > 193.204.161.49: icmp: time exceeded in-transit (ttl 251, len 56)
13:00:28.385546 193.204.161.49 > 193.204.5.26: udp 12 (ttl 5, len 40)
13:00:28.401666 193.206.134.230 > 193.204.161.49: icmp: time exceeded in-transit (ttl 251, len 56)
13:00:28.401764 193.204.161.49 > 193.204.5.26: udp 12 (ttl 5, len 40)
13:00:28.419377 193.206.134.230 > 193.204.161.49: icmp: time exceeded in-transit (ttl 251, len 56)
13:00:28.419503 193.204.161.49 > 193.204.5.26: udp 12 (ttl 6, len 40)
13:00:28.490897 193.206.131.54 > 193.204.161.49: icmp: time exceeded in-transit (ttl 250, len 56)
13:00:28.493087 193.204.161.49 > 193.204.5.26: udp 12 (ttl 6, len 40)
13:00:28.513827 193.206.131.54 > 193.204.161.49: icmp: time exceeded in-transit (ttl 250, len 56)
13:00:28.513928 193.204.161.49 > 193.204.5.26: udp 12 (ttl 6, len 40)
13:00:28.533381 193.206.131.54 > 193.204.161.49: icmp: time exceeded in-transit (ttl 250, len 56)
13:00:28.533507 193.204.161.49 > 193.204.5.26: udp 12 (ttl 7, len 40)
13:00:28.593957 193.204.5.26 > 193.204.161.49: icmp: 193.204.5.26 udp port 33453 unreachable (ttl 57, len 68)
13:00:28.595615 193.204.161.49 > 193.204.5.26: udp 12 (ttl 7, len 40)
13:00:28.673035 193.204.5.26 > 193.204.161.49: icmp: 193.204.5.26 udp port 33454 unreachable (ttl 57, len 68)
13:00:28.673146 193.204.161.49 > 193.204.5.26: udp 12 (ttl 7, len 40)
13:00:28.690380 193.204.5.26 > 193.204.161.49: icmp: 193.204.5.26 udp port 33455 unreachable (ttl 57, len 68)

58 packets received by filter
0 packets dropped by kernel
giga:~#
```

130-icmp-05 copyright ©2020 g. di battista, m. patrignani, m. pizzonia

24

studiare le reti di calcolatori è anche studiare i vari tool di supporto

arpwatch
tracertoute
(nei sistemi
Windows "tracert")
nslookup
tcpdump
wget
snort
trat
whois
ipconfig
nmap
ntop
dig
net-snmp
ping
bro
iperf
NDT
wireshark
dummynet
mrtg

130-icmp-05 copyright ©2020 g. di battista, m. patrignani, m. pizzonia